الجامعة اللبنانية
كلية الحقوق والعلوم السياسية والادارية
العمادة

الحوسبة السّحابية وحماية المعلومات

رسالة أعدّت لنيل دبلوم شهادة الماستر البحثي في قانون الأعمال

إعداد
أنطونيلا طوني شدياق

لجنة المناقشة

البروفيسور علي رحال	الأستاذ المشرف	رئيساً
الدكتورة جنان الخوري	أستاذ مساعد	عضواً
الدكتور محمود رمّال	أستاذ مساعد	عضواً

2019



الجامعة اللّبنانية غير مسؤولة عن الآراء الواردة في هذه الرسالة، وهي تعبر عن رأي صاحبها فقط.

مرّت السّنون ... وكبر الحلم

واستفاقت الآمال من تحت اليراع

وتعانقت الجهود ... فكان الإبداع

الإهداء

يا من أحمل اسمك بكل فخر

يا من فتحت لي الآفاق والدّروب

يا من أهديتني الحياة

أهديك هذا البحث

أبي

إلى من جرعت كؤوس الألم لتسقيني قطرة حب

إلى من حصدت الأشواك من دربي

ونثرت زهوراً لمدى العمر

أقدّم أول حفنة من حصاد الفكر

أمي

له كل **الشّكر**

أستاذي الذي نهلت من حصيلة فكره

فأنار دياجير الظلمات في فكري

البروفيسور **علي فايز رحال**

مقدمة

إنتقل الناس من العالم الحقيقي إلى العالم الإفتراضي، الذي يمكن إطلاق إسم العالم السّيبراني عليه، حيث معظم الخدمات المقدمة مبنية على السّحابة. لقد كانت الطريق طويلة للوصول إلى تقنية السّحابة، فيمكن إرجاع سجلّها إلى إختراع أول آلة حساب. في عام 1623 Wilhelm Schickard كان أول من قام بتوثيق تجميع آلة حساب كهذه. ومن ثم لعلّه في عام 1822 طوّر العالم Charles Babbage أول آلة أوتوماتيكية.

من المعالم البارزة الأخرى كان مشروع Allan Marquand لآلة المنطق الكهربائي عام 1885 وتم تطبيق هذه الآلة لأول مرّة في عام 1936 من قبل Benjamin Burack.

أمّا التاريخ الفعلي للكمبيوتر الحديث فقد بدأ عام 1941 ببناء Konard Zuse لجهاز Z3 الذي كان أول جهاز كمبيوتر رقمي. وفي عام 1945، قام كلّ من John Mauchley و J. Presper Eckert ببناء ENIAC وهو مكوّن عددي إلكتروني وكمبيوتر[1]. مع إختراع الترانزستور عام 1947 ظهرت التطورات في مجال الكمبيوتر بشكل لافت. قدّمت شركة IBM عام 1957 جهاز 704 كأول جهاز كمبيوتر مركزي مع نظام النقطة العائمة. وقد تبعه إستعمال نظام IBM/360 عام 1964. كان أبرز ما في هذه المجموعة المكونات القابلة للتبديل والبرامج القابلة للتنفيذ على جميع أجهزة الكمبيوتر من عائلة المنتج هذا.

أدّت التطورات المستمرة وتصغير أجهزة الكمبيوتر المركزية إلى الحصول على أجهزة مستقلة MINICOMPUTERS مثل PDP-8 عام 1964 أو Alto عام 1974[2]. بدأ تطوير الكمبيوتر الشّخصي (PC: Personal Computer) في أوائل السّبعينيات من القرن الماضي مع بناء أول معالج صغري 4004 عام 1969 ثم 8008 لاحقاً في عام 1971 بواسطة Intel. كان هذا الأخير الأساس لأول كمبيوتر منزلي Micral بواسطة André Thi Truong عام 1973[3]. ومن ثم تبعه العديد من أجهزة الكمبيوتر المنزلية مثل Apple، Atari و Commodore وغيرها.

---

[1] Goldstine, H.H., A. Goldstine. 1946. The electronic numerical integrator and computer (ENIAC). Mathematical Tables and Other Aids to Computation: 97-110.

[2] Freiberger, Paul, Michael Swaine. 2000. Fire in the valley: the making of the personal computer. 2. Ed. New York: McGraw- Hill.

[3] Supra 2

في وقت متأخر من عام 1981، دخلت شركة IBM هذا القطاع من السّوق وصاغت اسم الكمبيوتر الشّخصي Personal Computer. قامت Microsoft بتطوير نظام التشغيل لجهاز الكمبيوتر IBM، الذي سرعان ما أصبح النظام الأساسي القياسي مع العديد من شركات تصنيع أجهزة الكمبيوتر الشّخصية.[4] ومنذ ذلك الحين، اكتسب تطوير الكمبيوتر وانتشاره أهمية كبيرة، فالأداءات العديدة وإنشاء واجهات رسومية للمستخدم وتصغير الأجهزة أدّت إلى تطوير أجهزة الكمبيوتر المحمولة (laptop).

من المعالم المهمة الأخرى كان تطوير الإنترنت الذي يمكن إرجاعه إلى مشروع بحث في وكالة مشاريع البحوث المتقدمة (ARPA)[5]. تم تطوير نظام الإتصالات عام 1969 من قبل وزارة الدفاع الأمريكية، ومن خلاله تم تطوير ARPAnet. عام 1981 تم توصيل حوالي 200 مؤسسة بهذه الشّبكة. أمّا عام 1983 فقد تم تحويل protocol net إلى IP/TCP، مما أتاح توصيل الشّبكات الفرعية بالكامل بشبكة ARPAnet. هذه الشّبكة سرعان ما سميّت بالإنترنت التي كانت تستخدم في البداية للأغراض العسكرية والعلمية، وصارت منذ عام 1988 تسوّق مع خدمات مثل البريد والتلنت و usenet.[6]

حققت الإنترنت ظهورها الحقيقي عام 1989 مع اختراع Tim Berner Lee للشبكة العالمية (World Wide Web) وهي شبكة إرتباطات تشعبية لنظام إدارة المعلومات للمنظمة الأوروبية للبحوث النووية (CERN)[7]. مع الانتشار المتزايد لمستعرض الويب Mosaic، إكتسب World Wide Web في النهاية شعبية كبيرة[8]. زيادة تطور التقنيات مثل JAVA أو PHP أو AJAX جعلت من الممكن تطوير مواقع ويب أكثر تفاعلية. بسبب هذا التطور، يمكننا اليوم العثور على العديد من مواقع الوسائط والمتاجر عبر الإنترنت. ومن الأمثلة على ذلك، مخططو الطريق (route planners)، منصات الإتصال، الشّبكات الإجتماعية وكذلك تطبيقات للمكاتب كمعالجات النصوص أو تطبيقات النشر الورقية. إكتسب مفهوم النشر هذا، الذي يطلق عليه عادةً اسم Software-As-Service (SAS)، شعبية عام

---

[4] Supra 2

[5] ARPA: Advanced Research Projects Agency

[6] Supra 2

[7] CERN: European Organization for Nuclear Research

[8] Berners-Lee, Iim. Information Management: A proposal. World Wide Web Consortium, 1998-1989. (Available on: http://www.w3.org/History/1989/proposal.html).

2000.[9] تم تطوير مفاهيم نشر مماثلة لنشر موارد الأجهزة خاصةً طاقة الحوسبة والتخزين. في الأساس، كانت الحوسبة الشّبكية مطبقة وفق هذا المفهوم في الأوساط الأكاديمية. تمت صياغة مصطلح "الحوسبة السّحابية" في عام 2007 ويتم استخدامه للدلالة على مفهوم نشر الأجهزة والبرامج المشتركة.

تعتمد الحوسبة السّحابية على مجموعة من المفاهيم الموجودة مسبقاً والمدروسة جيّداً مثل الحوسبة الموزعة والشّبكات والمحاكاة الإفتراضية أو البرامج كخدمة (SAAS). على الرغم من أن العديد من المفاهيم لا تبدو جديدة، إلّا إن الإبتكار الحقيقي للحوسبة السّحابية يكمن في الطريقة التي يوفر بها خدمات الحوسبة للعملاء. بالإضافة إلى كل ما أتينا على ذكره، لعبت الحوسبة السّحابية دوراً مهماً في ما يسمى outsourcing أي الإستعانة بمصادر خارجية، فكانت الإستعانة بالسّحابة تقدم الكثير من الفوائد للشّركات والمؤسسات والأشخاص، أهمّها إنقاص التكلفة، فإعتمدت هذه الجهات على السّحابة لحفظ بياناتها ومعلوماتها.

غالباً ما تعتمد الوسائط والإعلان على السّحابة إلّا إنها ليست مناسبة لجميع المجالات. تتمثل العقبات الرئيسية في عدم توفر الخدمة بشكل كافٍ، وبيئات البرمجيات الإحتكارية، وقابلية المراجعة، ومشاكل سريّة البيانات واختناقات نقل البيانات عبر الشّبكة وعدم القدرة على التنبؤ بالأداء، وقضايا المسؤولية القانونية.[10] أمّا إشكالية حماية البيانات خاصةً تلك ذات الطابع الشّخصي طرحت في القرن الواحد والعشرين بكثرة بسبب الإختراقات العديدة التي جرت على الشّركات وبالأخص على البيانات المحفوظة لديها المتعلقة بخصوصية الأشخاص كأسمائهم وتواريخ ميلادهم والبريد الإلكتروني الخاص بهم وكلمات المرور حتّى أرقام بطاقات الإئتمان التي تعود لهم وغيرها من المعلومات التي يطغى عليها الطابع الشّخصي. فيمكننا إرجاع الخروقات الكبيرة إلى عام 2006 إذ تم إختراق شركات TJX Companies, Inc. وكُشِفَ عن 94 مليون بطاقة إئتمان، كذلك عام 2008 تم الكشف عن 134 مليون بطاقة إئتمان في شركة Heartland وعند إكتشاف هذا الخرق تم إعتبار هذه الشّركة غير متوافقة مع معيار أمان بيانات صناعة بطاقات الدفع (PCI DSS) وأوقفت الشّركة عن إجراء التحاويل لفترة من الزمن؛ فهذا الأمر بالإضافة إلى خرقه بيانات الأشخاص والتلاعب في بطاقاتهم وحساباتهم، يؤدي إلى

---

[9] Bennett, K, P Layzell, D Budgen, et al. 2000, Service-based software: the future for flexible software. In Seventh Asia- Pacific Software Engineering Conference (APSEC). Singapore.

[10] Armbrust, Michael, Armando Fox, Rean Griffith, et al. 2009. Above the Cloud: A Berkeley View of Cloud Computing. Berkeley: EECS Department, University of California.

فقدان الشّركات التي تم إختراقها الثقة وهذا له تأثير كبير على أكثر من صعيد. يمكننا ذكر الإختراقات التالية أيضاً:

- شركة Yahoo: كانت ربما ضحية لأكبر خرق بيانات في التاريخ، حيث في عام 2013، تم إختراق جميع حسابات المستخدمين البالغ عددها 3 مليارات، حسب تقدير الشّركة. لقد أدّى هذا الهجوم إلى تهديد الأسماء الحقيقية للمستخدمين وعناوين البريد الإلكتروني وتواريخ الميلاد وأرقام الهواتف. عقب هذا الهجوم إنخفضت قيمة الشّركة السّوقية التي كانت تقدر بمئة مليار دولار أميركي وتم تغيير إسمها بعد بيعها بقيمة 4.48 مليار دولار أميركي.[11]

- شركة FaceBook: إن أعداد الأشخاص الذين تأثروا بالخروقات على موقع فايسبوك، ومن المستحيل تحديد الخروقات جميعها من المرّة الأولى، قد تكلموا في الأول عن 87 مليون حساب، من ثم 30 مليوناً والآن 540 مليوناً وتستمر القائمة. هذه الخروقات أدّت إلى الحصول على الأسماء والبريد الإلكتروني وتواريخ الميلاد وكلمات المرور والتفاعلات والتعليقات التي شاركها صاحب الحساب مع غيره. وبمجرد الكشف عن هذه البيانات لا توجد طريقة لإستعادتها لأنه في لحظة يمكن نسخها وإعادة حفظها في مكانٍ آخر[12].

- تطبيق Whatsapp: الذي هو وحدة تابعة لـ FaceBook، خرق أمنياً في تطبيق الرسائل الخاص به، وكان الخرق باستخدام تطبيق مطوّر من قبل شركة خاصة تحت إشراف حكومي. لم يعرف عدد المستخدمين الذين طالهم هذا الإختراق مع لفت النظر إلى أن هذا التطبيق مستخدم

[11] Taylor Armerding: "The 18 biggest data breaches of the 21st centure", unknown date of publishing, published on csoonline.com.
(Available on: https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html) (Accessed on 5 May 2019, at 10:25 AM).

[12] APRIL GLASER: "Another 540 Million Facebook Users' Data Has Been Exposed", 03 April 2019, published on slate.com. (Available on: https://slate.com/technology/2019/04/facebook-data-breach-540-million-users-privacy.htnl) (Accessed on April 15, 2019 at 8:35).

من قبل 1.5 مليار شخص شهرياً. عقب ذلك طوّر هذا التطبيق وطلب update للحماية من هذا الخرق.[13]

هذه كانت من أهم الشّركات التي تهمّ المواطن اللّبناني والتي أظهرت عدم تمتعها بالسّرية والأمان اللّذين يظن المستخدم بتوافرها، فكانت عرضة لإختراقات عديدة طالت الكثير من المواطنين اللّبنانيين خاصةً تلك التي مسّت تطبيق FaceBook العام المنصرم. لكن لا تقتصر الإختراقات على هذه الشّركات إذ هناك عدد لا يحصى من الإختراقات حول العالم منها ما يطال عدداً كبيراً من المستخدمين وبعضها قد لا يطال سوى شخص واحد. هل في هذه الحالة الأخيرة تكون المسؤولية كما هي الحالة الأولى؟ فالإختراق هو إختراق حتّى لو لم يستطع المخترق الحصول على أيّة بيانات، ولكن احتمال وصوله إلى بيانات تمسّ بخصوصية صاحبها وارد. فبيانات الأشخاص والخصوصية التي يجب أن يتمتعوا بها وفق القوانين والمعاهدات والإعلانات العالمية لحقوق الإنسان هي من أهم المواضيع التي يجب التطرق إليها في موضوع السّحابة، فهذا الموضوع يطال العديد من الأشخاص: الشّخص الطبيعي الذي مسّت خصوصيته قد يتعرض للإبتزاز وغيره؛ الشّخص المعنوي الذي يقدم الخدمة التي تعرّضت للإختراق يفقد مصداقيته وسمعته بين المستخدمين وبين الشّركات التي تقدّم خدمة مماثلة، بالإضافة إلى نقص في القيمة السّوقية وتعرّض الإقتصاد القومي في البلد الموجود فيه إلى خلل. ومن أهمّ النتائج التي قد تصدر عن هذه الإختراقات، فرض شروط والتشديد على هذه الشّركات من قبل دولٍ أخرى خاصةً تلك التي يهمها حماية مواطنيها من أيّة خروقات والحفاظ على خصوصيتهم؛ خاصةً عندما يكون الإختراق مدعوماً من جهّة حكومية معيّنة هدفها الحصول على بيانات ناس موجودين في دول أخرى لأسباب سياسية أو غيرها.

في هذه الرسالة سنتكلم في بادئ الأمر عن السّحابة وتعريفها وتقريب مفهومها للمستخدمين. فهناك عدم معرفة أو حتـى رغبة بعدم المعرفة في ما يتعلق بكيفية عمل السّـحابة وكيفية الإشـتراك في الخدمـات وتأثيرها علينا، إذ إننا نقوم بنشر بياناتنا خاصةً الشّخصية منها في كل موقع نريد الدخول إليه غير مكترثين وجاهلين ما قد ينتج عنه من عواقب. حتى تاريخ إختياري موضوع هذه الرسالة جلّ ما كنت

[13] Katie Paul, Joel Schectman, Christopher Bing: "WhatsApp Security Breach May Have Targeted Human Rights Groups", 14 May 2019, published on reuters.com. (Available on: https://www.reuters.com/article/us-facebook-cyber-whatsapp/whatsapp-security-breach-may-have-targeted-human-rights-groups-idUSKCN1SK0SM) (Accessed on May 15, 2019 at 8:50 AM).

أقوم به هو إنشاء حسابات على مواقع التواصل الإجتماعي والنقر على كلمة موافق من دون قراءة شروط الإستخدام وأغلبية مستخدمي الإنترنت يقومون بالأمر عينه؛ لذلك من المهم أن نكون على بيّنة من حقيقة الأمور وحتى لو لم نكن من التقنيين، فإنه ليس من الضروري التعمق في الأمور التقنية.

وللسّحابة مزايا وفوائد عديدة أدّت لاكتسابها الأهمية التي هي عليها اليوم، أهمّها تقليل التكلفة إذ إنّها تغني عن عمليات عديدة مثل شراء الأجهزة والبرامج، السّرعة الهائلة في نقل المعلومات أو الحصول عليها مجدّداً، إنجاز الأعمال دون الحاجة إلى برامج إدارة الأعمال ودون الحاجة إلى مكان لتخزين الوثائق، كما إنّها تقوم بتخزين نسخ إحتياطية للبيانات كمزيد من الأمان، كلّ هذا يثير أسئلة من الضروري الإجابة عليها.

الأسئلة التي قد ترد إلى ذهن المستخدم والتي يكون لديه الفضول لمعرفتها تقع ضمن حماية البيانات، فأين تحفظ البيانات المتعلقة بالفرد؟ هل الفرد هو الوحيد الذي تحفظ بياناته؟ هل تختلف طرق إشتراك الفرد بالخدمة التي تحفظ بياناته عن غيره من الأشخاص؟ هل الإشتراك في هذه الخدمة هو الطريقة الوحيدة لحصول طرف ثالث على بياناته؟ أين يحتفظ هذا الطرف بالبيانات؟ هل هناك من طرق يمكن للشخص حماية بياناته بالرغم من الإحتفاظ بها لدى جهة أخرى؟ ما هي المخاطر التي قد يواجهها الفرد عند حصول أطراف أخرى على بياناته الشّخصية؟ كذلك ما هي الحماية التي يؤمنها له القانون اللّبناني؟ هل هذه الحماية فعّالة لمواجهة التطور الحاصل؟ ما هي النواقص في القانون اللّبناني مقارنةً مع القوانين الأجنبية التي تصب إهتمامها وخبراتها التقنية والقانونية في موضوع حماية البيانات؟ والسّؤال الذي يجب طرحه إلّا أن الجواب عليه بديهي جدّاً خاصةً بعد هذه الدراسة: هل من الآمن أن تكون متصلاً بالإنترنت في لبنان؟

IS IT SAFE TO BE ONLINE IN LEBANON?

بالتالي سيتعرف القارئ في القسم الأول على مفهوم السّحابة التي يتم الإحتفاظ بالبيانات فيها، وعلى إستخدامات هذه التقنية والطبيعة القانونية لها؛ كذلك كيفية إبرام العقد للإنتفاع منها والحماية المقررة للمستخدمين الذين يعتبرون مستهلكين، بعد تعريف المستهلك في إطار الحوسبة السّحابية. أمّا القسم الثاني سيعالج العقبات التي تعترض هذه التقنية من مشاكل تقنية إلى مشاكل قانونية تدخل خاصةً في نطاق إعتراض خصوصية المستخدم وتشكل الشّاغل الرئيسي للعديد من الدول خاصةً الإتحاد الأوروبي، فهو من الناشطين في العمل على حماية البيانات الشّخصية للأشخاص الذين تربطهم علاقة بدول الإتحاد، بينما دول أخرى على رأسها الولايات المتحدة تسعى بشتّى الطرق للوصول إلى أكبر عدد ممكن

من البيانات في أي دولة وجدت، ولكن يبقى معرفة مدى نجاحها في ذلك. بالإضافة إلى طرق حل النزاعات في حال نشوء نزاع في ما يتعلق بتنفيذ العقد، كذلك المسؤولية التي يتحملها مزوِّد الخدمة. كلّ ذلك عبر المقارنة بين قوانين أوروبية وأميركية وبالطبع التكلم عن القوانين اللّبنانية مسلطين الضوء على المحاولات الخجولة التي جرت في لبنان والتي كان أولها وأهمها عام 2018 أي بعد مرور 27 عاماً على بدء إستعمال الإنترنت بين الناس، ويعتبر ذلك إهمالاً من قبل المشرع لأمر أضحى أساسياً في حياة اللّبنانيين وسبب العديد من الجرائم الجديدة وسهّل البعض الآخر منها على سبيل المثال الإعتداء على البيانات المتعلقة بالأفراد، إستغلال الإنترنت لنشر الأفكار الإرهابية المنحرفة، كما ويمكننا ذكر تسهيل القدح والذم والإبتزاز وغيرها من الجرائم التي لن تكون محور الدراسة ولن نتطرق إليها سوى بأفكار قد ترد في بعض الفقرات إلّا في ما يتعلق بالولوج إلى البيانات التي هي من ضمن هذه الدراسة.

قسّمت الدراسة إلى قسمين وفق ما يلي:

القسم الأول: الإطار القانوني للحوسبة السّحابية

الفصل الأول: مفهوم الحوسبة السّحابية

المبحث الأول: ماهية الحوسبة السّحابية

المبحث الثاني: تمايز الحوسبة السّحابية

الفصل الثاني: كيفية إبرام عقد الحوسبة السّحابية

المبحث الأول: توافرية خدمات الحوسبة السّحابية وفق حاجات ومتطلبات المستهلك

المبحث الثاني: إبرام العقد وحماية المتعاقد الضعيف

القسم الثاني: المخاطر والعوائق التي تواجه الحوسبة السّحابية

الفصل الأول: المخاطر التقنية

المبحث الأول: الثقة في المزوِّد

المبحث الثاني: السّرية في الحوسبة السّحابية

الفصل الثاني: الحماية القانونية للبيانات

المبحث الأول: الحق في الخصوصية وتبعاتها

المبحث الثاني: حل النزاعات الناتجة

القسم الأول: الإطار القانوني للحوسبة السّحابية

الحوسبة السّحابية مصطلح قد يبدو غريباً للوهلة الأولى، إذ لم تعتد الأذن في هذه الأيام على سماع مصطلحات تقنية باللّغة العربية. لكن من المهم فهم هذا المصطلح خاصةً من الناحية القانونية والتقنية إذ إنه غدا أمراً أساسياً في الحياة اليومية لكل فرد كما للأشخاص المعنويين والحكوميين. هناك شركات عديدة تقدم هذه الخدمة إذ إن لها العديد من المزايا؛ كما من الممكن تقديم الخدمة من قبل أشخاص ثالثين أي وسطاء بين الطرفين الأساسيين لهذه العلاقة ومن الضروري معرفة التصنيف القانوني لهم. هذه الخدمة تعطي المستخدم حريّة إختيار نوع الخدمة التي يريدها إذ أنها تقدمّ بعدّة أشكال. العلاقة التي تربط المزوِّد بالمستخدم لها طبيعة خاصة بها يجب التطرق إليها لتحديد إذا ما كانت علاقة تعاقدية أم غيرها فذلك يؤدي إلى إختلاف المسؤولية المترتبة على كل طرف. ويبقى أن نطرح الأسئلة التالية التي سنقوم الإجابة عليها أيضاً في هذا القسم. ما الذي يفرق هذه التقنية عن غيرها من التقنيات؟ ما الذي تقدمه؟ كذلك ما الذي يميّزها عن غيرها من العقود القانونية؟ وكيفية إبرام العقد المتعلق بها وماهي الحماية القانونية المتوفرة في إطار هذا التعاقد؟

الفصل الأول: مفهوم الحوسبة السّحابية

يجب في بادئ الأمر فهم معنى هذا المصطلح ومعرفة مزايا هذه التكنولوجيا؛ كذلك دراسة من يقوم بتقديم هذه الخدمة أو هذه التكنولوجيا، وما هي الطبيعة القانونية لهذا الشخص. ومن الضروري تصنيفها من الناحية القانونية بالإضافة إلى تفريقها عن غيرها من المصطلحات التقنية والأشكال القانونية.

المبحث الأول: ماهية الحوسبة السّحابية

في هذا المبحث الأول، سنتكلم بشكل عام عن الحوسبة السّحابية وتعريفها وإيراد مزاياها كفكرة عامة لتوضيح بعض الالتباسات لدى الأشخاص. كما سنشير إلى أهم الشّركات العالمية والمحلية التي تقدم خدمة الحوسبة السّحابية ودورها وإظهار ما إذا كانت العلاقة التي تربط بين المزوّد والعميل هي علاقة مباشرة أم من الممكن أن يكون هناك طرف ثالث، كما سنتكلم عن العلاقة بحد ذاتها وعن طبيعتها القانونية.

الفقرة الأولى: فكرة عامة عن الحوسبة السّحابية

عند إيراد كلمة حوسبة سحابية بين الأشخاص، قليل من يفهم معنى الكلمة أو يعرف ماذا تمثل، إذ إن جميع الأجيال الحديثة لديها فكرة عامة عن الـ Cloud كما أنها تستخدمها في حياتها الشخصية واليومية، ولكن هذه الفكرة العامة ليست واضحة، لذلك في هذه الفقرة سنقوم بتعريف الحوسبة السّحابية وبالتالي جعلها أكثر وضوحاً للكثيرين، كذلك ذكر أهم فوائدها ومزاياها التي كانت سبباً أساسياً لانتشارها.

النبذة الأولى: تعريف الحوسبة السّحابية

الحوسبة السّحابية مصطلح تقني قليل من سمع به أو فهم معناه: هو ترجمة حرفية لمصطلح "cloud computing" في اللّغة الإنكليزية أو مصطلح "infonuagique" في اللّغة الفرنسية: كثرت الترجمات لهذا المصطلح من السّحابة الحوسبية أو الغمامة الحوسبية أو السحابية الالكترونية ولكن اعتمد مصطلح الحوسبة السّحابية. فالحوسبة أي computing بالإنكليزية هو تطوير واستخدام تقنية الحاسوب[14].

أما السّحابة أي cloud بالإنكليزية هي عبارة عن غيوم أو غمام في السّماء الطبيعية ولكن في الحقيقة في إطار دراستنا السّحابة ليست السّحابة العادية بل هي عبارة عن سحب إلكترونية يتم فيها تخزين البيانات بشكل نبضات كهربائية يتم الوصول إليها عن طريق الإنترنت من خلال جهاز آلي أو أي جهاز له المقدرة على الإتصال بالإنترنت[15].

يثار النقاش عادةً حول تعريف الحوسبة السحابية، فكلما اقتربت المعايير والتعاريف لتحديدها، تتطور الخدمات وتتغير وتتسع مما يفاقم من جديد عدم توحيد تعريفها[16]. هذا ما يعرقل وضع إطار قانوني وتشريعي واضح، مما يسمح تعدد تعريفاتها. نذكر بعض هذه التعريفات:

- عرفها الإتحاد الدولي للإتصالات على أنها: "نموذج لتمكين مستخدمي الخدمات من النفاذ الشامل والمريح وتحت الطلب إلى مجموعة مشتركة من موارد الحوسبة القابلة للتغيير التي يمكن توفيرها على وجه السّرعة وإطلاقها بأقل جهد إداري أو تدخل من جانب مقدّم الخدمة"[17].
- أمّا المعهد القومي الأمريكي للمعايير والتكنولوجيا (NIST)[18] فقد قدّم تعريفاً كلاسيكيّاً واسعاً يظهر العناصر والخصائص الرئيسية للحوسبة السحابية، فعرّفها:

---

[14] LONGMAN Active Study Dictionary Of English, definition of computing: the activity or skill of using a computer, page 150.

[15] التعريف موجود على: https://dictionary.cambridge.org/fr/dictionnaire/anglais/cloud-computing

[16] جنان الخوري، **الحوسبة السّحابية في الدول العربية، الجوانب القانونية والتشريعية واقع وآفاق**، تقرير الاتحاد الدولي للاتصالات، بيروت، 2015، ص. 6.

[17] الاتحاد الدولي للاتصالات: السّلسلة **X: شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن**، التوصية ITU-T X.1601، 2014، ص.4.

[18] National Institute of Standards and Technology كان بين عام 1901 وعام 1988 معروفاً بالمكتب الوطني للمعايير. هو مختبر معايير القياس ووكالة غير اعتيادية لإدارة التجارة في الولايات المتحدة. المهمة الرسمية تشجيع الابتكار في الولايات المتحدة والقدرة التنافسية الصّناعية من خلال تطوير علم القياس والمعايير والتقنيات في السّبل التي تعزز الأمن الاقتصادي وتحسين نوعية الحياة.

“cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction[19]”.

أي أنها نموذج للتمكن من الوصول من كل مكان، بشكلٍ مريح كما وعند الطلب لمجموعة مشتركة من موارد الحوسبة التي تمت تهيئتها مثل (الشبكات والخوادم، وحدات التخزين والتطبيقات...) ويمكن توفيرها وإطلاقها بسرعة وبأقل جهد إداري أو تفاعل موفر الخدمة.

- كما وأن تعريف المنظمة الدولية للمعايير ISO[20] مماثلٌ لتعريف NIST:

"Cloud computing is a paradigm for enabling network access to a sealable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand”[21]

فاختارت تسميتها بال "evolving paradigm" أي النموذج المتطور.

- يمكننا ذكر تعريف آخر يشمل العديد من الخصائص الرئيسية للحوسبة السحابية ويقدم وجهة نظر أوسع وعمليّ لها أكثر:

“Clouds [are] a large pool of easily usable and accessible virtualized resources such as hardware, development platforms and or services. These resources can be dynamically reconfigured to adjust to a variable food (scale), allowing also for an optimum resource utilization. This pool of resources is typically exploited by a pay-per-use model in which guarantees are offered by the

---

[19] Peter Mell, Timothy Grance: **The NIST Definition of Cloud Computing**, NIST special publication 800-145, 2011, page 2.

[20] International Organization of Standardization منظمة غير حكومية أسست بتاريخ 23 شباط 1947، تعمل على وضع المعايير كما وتصرح عن معايير تجارية وصناعية عالمية التي يمكن أن تتحول الى قوانين إمّا عن طريق المعاهدات أو المعايير القومية.

[21] ISO/IEC DIS 17789:2014, **Information Technology- Cloud Computing- Reference Architecture**, 1st Edition, published on iso.org, 2014.

(Available at: https://www.iso.org/standard/60545.html?browse=tc) (Accessed on September 23, 2018; at 10:38 AM).

infrastructure provider by means of customized SLAs [service-level-agreements][22]."

فالغيوم هي مجموعة كبيرة من الموارد الإفتراضية التي يسهل استخدامها والوصول إليها مثل الأجهزة والمنصات و/أو الخدمات... والتي يمكن إعادة تشكيلها ديناميكياً للتكيف مع الحمل المتغير ممّا يسمح الإستخدام الأمثل للموارد. وعادةً ما يتمّ استغلال هذه المجموعة من الموارد من خلال نموذج الدفع لكل استخدام حيث يتم تقديم الضمانات من قبل مزود البنية التحتية من خلال اتفاقيات مستوى الخدمة المخصصة SLA.

يمكننا الاستخلاص من جميع هذه التعاريف أن الحوسبة السّحابية هي نموذج يسمح للشخص الطبيعي أو المعنوي بالحصول على المعلومات التي يريدها أكانت بيانات شخصية أو غيرها، أينما كان، متى أراد، بشكل سريع وبمرونة عالية وفق طلبه، سواء كان يحتفظ بهذه المعلومات بسحابة لديه أو لدى غيره. وعليه، استخلاصاً من كافة هذه التعاريف، يمكن استنتاج مزايا عديدة للحوسبة السّحابية تزداد أهميتها إذا كانت خدمة مقدمة من طرف آخر.

يجب الإشارة إلى أن جميع التعاريف المذكورة هي تعاريف تقنية إذ إن الحوسبة السّحابية هي أساساً فكرة تقنية ولكن إنتشارها والأهمية التي هي عليه اليوم فرضت واجب دراستها من الناحية القانونية خاصةً مع جميع الإشكاليات التي تثيرها، لذلك سنقدم تعريفاً قانونياً لهذا المصطلح لاحقاً.

النبذة الثانية: مزايا الحوسبة السّحابية

الحوسبة السّحابية هي تكنولوجيا انتشرت بسرعة ودخلت شتّى المجالات: الحياة الشّخصية، الحياة المهنية والحياة الحكومية كما سنرى لاحقاً عند مناقشة استعمالات هذه التقنية. واكتسبت أهميتها لكثرة مزاياها الموحدة في الاستعمالات الثلاثة السّابق ذكرها. فالسّحابة ليست مجرد حل تقني بل إنّها شكل من أشكال الحوسبة التي تعمل على تحسين تنفيذ الأعمال والتي تؤثّر على الأعمال بشكل إيجابي.

يمكننا ذكر مزايا السّحابة من المسح الذي أجرته تكسوب جلوبال[23] عام 2012:

1. الإدارة
- الوصول للبرمجيات بشكل أسهل
- التعافي من الكوارث بشكل أسهل

[22] Sam Murugesan and Irena Bojanova, "Cloud Computing: An Overview", published in **Encyclopedia of Cloud Computing**, John Wiley & Sons Ltd., United Kingdom, 2016, p. 3-14.

[23] Techsoup Global التي تأسست عام 1987 تحت اسم CompuMentor وهي شبكة دولية غير ربحية من المنظمات غير الحكومية وتقدم الدعم التقني والأدوات التكنولوجية إلى المنظمات غير الربحية الأخرى.

- تقليل أعباء إدارة النظام
- سرعة الإنتشار

2. التكلفة
- انخفاض استثمار رأس المال
- الاحتياج الى عدد أقل من موظفي تكنولوجيا المعلومات
- تحويل المصاريف الرأسمالية إلى مصاريف تشغيلية (IT)

3. الشّراكة
- تحسين التعاون
- سهولة الشراكة مع المؤسسات الأخرى

4. البيانات
- تحسين أمن البيانات
- تحسين تنظيم البيانات
- التحكم بالبيانات ومراقبتها[24]

وأكثر المزايا شيوعاً يمكن تلخيصها وشرحها كالآتي:

1. المرونة: نطاقها عريض أكثر من المعتاد، والخدمة المعتمدة عليها تعمل بشكل فوري على تلبية الطلب بسبب السّعة الكبيرة للخوادم العاملة عن بعد في تقديم الخدمة.
2. التعافي من الكوارث: عندما يعتمد الأشخاص على الخدمات المبنية على الحوسبة السّحابية، فلن يلزم الأمر وجود خطط للتعافي من الكوارث وحماية بياناتهم منها، فمزوّدو الخدمة يضعون معظم المسائل والإشكاليات في اعتبارهم ويعملون عليها بسرعة.
3. التحديثات الأوتوماتيكية للبرامج: مورّدو الحوسبة السّحابية يقومون بإجراء الصّيانة بأنفسهم من ضمنها التحديثات، وهذا يوفّر على العميل الكثير من الوقت ومن الخبرات التقنية.
4. توفير المصاريف الرأسمالية: إن خدمات السّحابة عبارة عن خدمات تقدم بنظام الدفع أثناء الإستخدام (pay-as-you-go)، ولذلك لا تدعو الحاجة لتخصيص مصاريف رأسمالية مقدماً.

---

24 TechSoup: **cloud computing: benefits and barriers for non profits & libraries**, 2012 (Available at: http://www.techsoup.org/SiteCollectionDocuments/Webinar-cloud-computing-benefits-and-barriers-2012-10-11-presentation.ppt) (Accessed on August 25, 2018; at 11:30 AM).

ولأنها أكثر سرعةً في الانتشار، فان تكلفة تشغيل المشاريع التجارية تقل بينما تستفيد من المصاريف التشغيلية المستمرة المتوقعة.

5. زيادة التعاون: تعمل هذه الخدمة على زيادة التعاون عن طريق السّماح للموظفين، أينما كانوا، أن يتصلوا بشبكة الإنترنت وأن ينفذوا أعمالهم بشكل متزامن على المستندات والتطبيقات التي يتم تداولها كما أن بإمكانهم أيضاً السّماح للزملاء وأقسام السّجلات بالحصول على التحديثات الهامة في وقت حقيقي.
6. العمل من أي مكان: طالما أن الموظفين يتوافر لديهم الوصول إلى شبكة الإنترنت، فإن بإمكانهم العمل من أي مكان. وقد توصلت إحدى الدراسات إلى أن نسبة 42% من العاملين البالغين قد يقبلون بالتنازل عن جزء من راتبهم إذا تم السّماح لهم "بتنفيذ أعمالهم عن بعد" وغالباً ما يكون من المنزل، وفي المعدّل المتوسط قد يقبلون استقطاعاً من الراتب بمعدل 6%.[25] وبالنسبة للمعلومات الشخصية المتعلقة بحياة الفرد الشخصية، فيمكنه أيضاً الوصول إلى المعلومات التي يريدها أينما كان.
7. مراقبة المستندات: في الشركات التي لا تستخدم الحوسبة السّحابية، يقوم الموظفون في المعتاد بإرسال وتداول ملفاتهم عبر البريد الإلكتروني، بمعنى أن شخصاً واحداً فقط يمكنه أن يعمل على ملف في المرة الواحدة، ويحمل المستند العديد من أسماء الأشخاص والصّيغ والإصدارات. تسمح السّحابة بأن يتم الإحتفاظ بكافة الملفات في موقع مركزي واحد، ويمكن للجميع العمل من نسخة مركزية واحدة. وبإمكان الموظفين التواصل مع بعضهم البعض أثناء إجراء التغييرات. وهذه العملية بأكملها تجعل التعاون أكثر قوة، مما يزيد بدوره من الفعالية في الشّركة.
8. الأمن: في كل عام، تفقد مئات الآلاف من أجهزة الكمبيوتر المحمولة في المطارات حول العالم. الأجهزة الشّخصية، الأجهزة التي تعود ملكيتها للشركة، كلّها محملة بمعلومات شخصية، حسّاسة، مهنية... ومن الممكن أن يشكل ذلك خسائر مالية جسيمة بالإضافة إلى مسائل أمن البيانات، ولكن عندما يتم تخزين كل شيء في السّحابة، يكون من الجائز والسّهل الوصول إلى البيانات بغض النظر عمّا يحدث للجهاز بحيث أن البيانات لا يتم تخزينها بشكل مادي على الجهاز المفقود.
9. عدم تلويث البيئة: إن المشاريع والأشخاص الموجودين على الحوسبة السّحابية، يستخدمون فقط مساحة معيّنة من الخادم مما يقلل من استهلاك الطاقة، إذ لا يستخدم كل شخص معنوي أو

[25] SalesForce: **Why move to the cloud? 10 Benefits of cloud computing**, 2015; 6th point: work from anywhere. (Available at: https://www.salesforce.com/uk/blog/2015/11/why-move-to-the-cloud-10-benefits-of-cloud-computing.html) (Accessed on August 25, 2018; at 12:00 PM)

طبيعي الطاقة لتشغيل الخوادم لديه، فهناك مركز أو عدّة مراكز لشركة أو أكثر توجد فيها الخوادم وهذا أفضل من أن يكون لكل شخص طبيعي أو معنوي مثل هذا المركز. [26]

الفقرة الثانية: ماهية مزودي خدمة الحوسبة السّحابية وطبيعة العلاقة بين المزوِّد والمستخدم

بما أننا رأينا مسبقاً أن العميل يمكن أن يكون إمّا شخصاً طبيعياً أو شخصاً معنوياً أو حتى شخصاً حكومياً فسنقوم بالبحث مفصلاً عن استعمالات كل من هذه الأطراف على حدة، إلّا إننا سنظهر في هذه الفقرة مزودي الخدمة والوسطاء ما بين طرفي العلاقة السّحابية، كذلك العلاقة التي تربطهم بالعميل والطبيعة القانونية لهذه العلاقة حيث تختلف المسؤوليات وطرق الإثبات وغيرها باختلاف طبيعة العلاقة.

النبذة الأولى: مزود خدمة الحوسبة السّحابية

سنوجز الحديث عن أهم الشّركات التي تقدم خدمة السّحابة والتفرقة ما بين مزودي الخدمة والأشخاص الوسطاء بين الشركات الأساسية المزودة والعملاء وأهمية تواجدهم، كذلك والطبيعة القانونية لهؤلاء الوسطاء.

البند الأول: الشركات مزوّدة خدمة الحوسبة السّحابية مباشرة

تقليدياً، يحتفظ الشخص ببياناته ومعلوماته على حاسوبه أو بطرق تقليدية، إذا كانت الشركة ذات أهمية فيمكنها تأسيس سحابتها الخاصة وإنشاء مركز بيانات خاص بها (Data Center) أو الاشتراك بخدمة الحوسبة لدى مزوّد. مزوّد خدمة الحوسبة السّحابية (CSP)[27] هو شخص طبيعي أومعنوي، غالباً ما يكون شخصاً معنوياً، يقدم خدمات الشبكة أو البنية الأساسية أو تطبيقات الأعمال في السّحابة، بالإضافة إلى خدمات مكملة أو تابعة لخدمة السّحابة. يجب توافر صفات عديدة في المزوّد، كفهم آلية العمل، توفير المعلومات والدعم المطلوب، تقدير التكلفة مقابل الاستخدام وتوفير معايير الأمان وقابلية التوسع.

الحوسبة السّحابية هي فكرة أو مشروع يجب أن يتجسد بشكل قانوني وفق ما يختاره صاحب هذه الفكرة تطبيقاً لقوانين البلد الذي يريد إنشاء المشروع فيه. فمثلاً في لبنان وفق القوانين المرعية الإجراء وبالأخص قانون التجارة البرية اللّبناني، يمكن للمزود أن يختار العمل ضمن إطار مؤسسة أو شركة.

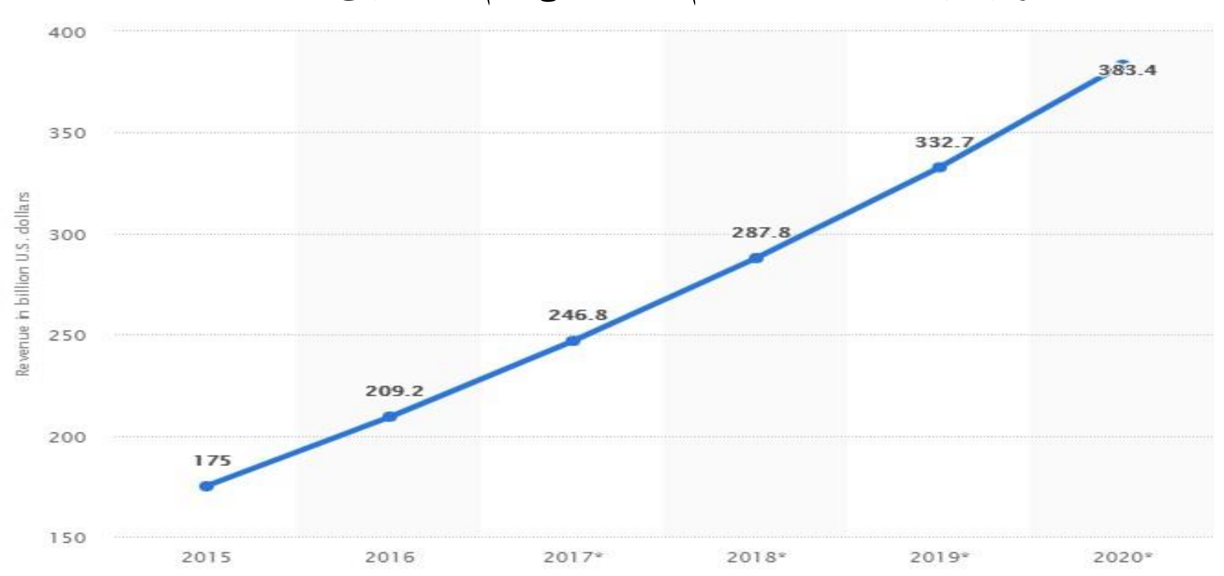
حالياً يتناول قانون التجارة اللّبناني عدّة أنواع أو أشكال من شركات الأموال التجارية التي لا تقوم على الإعتبار الشّخصي للشركاء، وغالباً ما تكون هذه الشركات من شركات الأموال لضخامة رأسمالها

---

[26] Supra 25.

[27] CSP: Cloud Service Providers

ومردودها وأهميتها، ففي احصاءات أجرتها شركة statista عام 2017 تظهر كيفية تطور سوق خدمات الاستضافة المدارة والحوسبة السّحابية من عام 2015 حتى عام 2020 وفق:[28]



يمكننا ذكر شركة مساهمة للحوسبة السّحابية مؤَسّسة في لبنان، حيث أن بيانات عملائها موجودة في لبنان، فالسّحابة موجودة في لبنان، إذ إن الشّركة موضوعها تقديم خدمة الحوسبة السّحابية وليس التوسط بين العميل وشركة سحابية موجودة خارج لبنان، فلا تطبق عليها سوى القوانين اللّبنانية المرعية الإجراء، وهي شركة Cirrus التي تشكل جزءاً من ITG (Holding)[29]، تقدم مجموعة شاملة من خدمات الحوسبة السّحابية وحوسبة الخدمات المدارة على مستوى المؤسسات[30].

كذلك جاء في قانون المعاملات الالكترونية والبيانات ذات الطابع الشّخصي 2018/81 على أن مقدم الخدمات التقنية يعتبر متخذ محل إقامة قانوني في لبنان عندما يكون مستقراً فيه بصورة دائمة لممارسة نشاطه أيّاً كانت جنسيته وأيّاً كان مركزه الرئيسي في حال كان شخصاً معنوياً.[31]

كما يمكننا ذكر العديد من الشّركات العالمية التي نستخدم خدماتها يومياَ، أهمها وعلى سبيل المثال:

1. شركة Google
2. شركة Amazon
3. شركة Microsoft

---

[28] Cloud computing market revenues worldwide from 2015 to 2020 (in billion U.S. dollars) (Available on: https://www.statista.com/statistics/270811/cloud-computing-revenue-worldwide-since-2008/) (Accessed on August 25, 2018; at 12:32 PM)

[29] Information Technology Group: شركة هولدنغ لبنانية وعضو في HOLCOM Group الذي يتضمن أكثر من 200 شركة في 35 بلد، والذي بدأ العمل بها منذ عام 1967.

[30] www.itgholding.com/affiliate/4/cirrus (Accessed on August 25, 2018; at 4:06 PM).

[31] المادة 75 من قانون المعاملات الإلكترونية والبيانات الشخصية رقم 2018/81.

1. شركة Google

Google هي أيضاً واحدة من بين مقدمي خدمات السّحابة الرائدين الذين يوفرون تخزيناً آمناً لبيانات المتسخدم. إنها تقدم منصة سحابية Cloud Platform، محرك تطبيق App Engine، سحابة للطبع Cloud Print، سحابة اتصال Cloud Connect، والعديد من الميزات المتطورة الموثوقة والتي تتمتع بالأمان. هذه الشركة تقدم الكثير من هذه الخدمات مجاناً أو بأقل تكلفة مما يجعلها سهلة الاستخدام.

2. شركة Amazon

AMAZON WEB SERVICES (AWS) هي عبارة عن مجموعة من خدمات الحوسبة عن بعد التي تشكل منصة حوسبة سحابية تقدم عبر الانترنت عبر Amazon.com. الخدمة الأكثر مركزية وشهرة من بين خدمات Amazon للحوسبة هي Amazon Elastic Compute Cloud (Amazon EC2) والتي تتيح للمستخدمين تأجير الماكينات الإفتراضية والتي يقومون بتشغيل تطبيقات الحاسب الخاص بهم عليها[32] .

3. شركة Microsoft

لم تعِ Microsoft إلّا مؤخراً فكرة أن الحوسبة السّحابية أصبحت جزءاً ضرورياً تتجه إليه الشّركات والأفراد لتعدد مزاياها. فأطلقت Azure المنصة السّحابية التي تمكن المطورين أن يبرمجوا نفس التطبيقات التي تعمل على نظام تشغيل windows لتعمل على السّحابة.

البند الثاني: سماسرة/وسطاء الحوسبة السّحابية

مع توسع خدمة الحوسبة السّحابية وانتشارها واعتمادها من قبل الشّركات والأفراد، ظهر وسطاء السّحابة لمساعدة مزودي الخدمة على تقديمها للعملاء.

أولاً: تعريف سمسار السّحابة ودوره

سمسار السّحابة هو منظمة وسيطة مهمتها تبسيط العلاقة بين مزود الخدمة والمستخدم. يجمع السّماسرة الخدمات ويدمجونها ويخصصونها للعملاء وهو أمر غالباً ما يواجهه مقدمو الخدمات السّحابية.

---

[32] أياد عماد علي: **الحوسبة السّحابية**، البنك المركزي العراقي دائرة تقنية المعلومات والاتصالات، منشور على cbi.iq. (يمكن إيجاده على cbi.iq/static/uploads/up/file-152377270192790.pdf، تم مراجعة الموقع بتاريخ 30 آب 2018 الساعة 11:52 قبل الظهر).

إن عدم وجود وسيط بين مزوّد السّحابة والمستهلكين يسبب استهلاكاً أكبر للوقت والعمل والنفقات، فشركة واحدة قد تستخدم Google Apps للبريد الالكتروني و Salesforce.com للمبيعات وخدمات Amazon Web Services لخدمات النظام الأساسي. يسهّل الوسيط السّحابي على كل من هؤلاء المزودين تقديم قيمة لعملائهم مع تمكين العميل أيضاً من تنسيق هذه الخدمات[33].

ويمكننا تلخيص الأدوار التي يلعبها الوسيط السّحابي بثلاثة أدوار رئيسية:

1. **Aggregation** أي **التجميع** بمعنى أنه يمكن للوسيط السّحابي تجميع العديد من الخدمات الفردية معاً وتقديمها كخدمة موحدة.
2. **Integration** أي **التكامل** فغالباً ما تعتمد المؤسسة على وسيط السّحابة لتحقيق التكامل بين خدمات متعددة. مما يوفر وظائف جديدة بشكل جماعي: يمكن أن يساعد وسيط السّحابة مثلاً على نقل البيانات إلى السّحابة ودمج شبكة العميل مع شبكة المزوّد.
3. **Customization** أي **التخصيص** فغالباً ما يقوم وسيط السّحابة بتخصيص الخدمات السّحابية للعملاء الفرديين نظراً لأنه لا يمكن تغيير الخدمات السّحابية إلّا من خلال مزود الخدمة[34].

وبالتالي للوسيط منافع عدّة: يساعد في الحفاظ على العلاقة بين المزود والعميل، يقوم بتنفيذ الخدمات والحلول التي قد لا تكون جزءاً من الإتفاقيات الأساسية الخاصة بمزود الخدمة (SLA)، ويجمع بين القوة الشّرائية للمؤسسات المتعددة، والتفاوض على أسعار أفضل للعملاء مع تقديم المزيد من العملاء إلى المزوّد. وقد يحق لسماسرة السّحابة في بعض الأحيان التفاوض على العقود مع مقدمي الخدمات السّحابية نيابة عن العميل. في مثل هذه الحالات، يتم منح الوسيط سلطة التعاقد على الخدمات عبر العديد من البائعين والتي يمكن أن تكون استراتيجية ممتازة للحفاظ على انخفاض التكاليف. بالإضافة إلى ذلك، عادةً ما تكون لدى شركات الخدمات المشتركة علاقات موجودة مسبقاً مع عدد من الموردين، وفي بعض الحالات يكون لديها عقود محددة مسبقاً، مما يساعد على تسريع عملية البيع[35].

---

[33] Lisa Sampson: **A cloud broker can be a cloud provider's best friend**, January 2012, (Available on: https://searchitchannel.techtarget.com/feature.com/feature/A-Cloud-Broker-Can-Be-A-Cloud-Providers-Best-Friend) (Accessed on August 26, 2018; at 10:38 AM).

[34] Talkin' Cloud: **Cloud Services Brokerage Company List and FAQ**, published on channelfutures.com March 13, 2015. (Available on: https://www.channelfutures.com/business-models/cloud-services-brokerage-company-list-and-faq) (Accessed on August 26, 2018; at 11:05 AM).

[35] Stephan Watts: **Cloud Service Brokerages: How CSB's Fit in a Multi-Cloud World**, published on bmc.com, August 21, 2017. (Available on: https://www.bmc.com/blogs/cloud-service-brokerages-how-csbs-fit-in-a-multi-cloud-world/) (Accessed on August 28, 2018; at 13:10 PM).

وأهم هذه المنافع في عمل الوسيط تقليل المخاطر والمخاوف الأمنية، الأمر الذي لا يزال يقلق مزودي الخدمات السّحابية والوسطاء والعملاء على حدّ سواء. ووفقاً لـ Greg Young أحد المحللين الأمنيين في Gartner[36]، إن اكتشاف التسلل يساعد على تخفيف التهديدات، لكن مسؤولي النظام يقولون إن عدم قدرتهم على مراقبة ومعالجة مشاكل الأمان السّحابية قبل أن تصل إلى الشّبكة هي أكبر مشكلة لديهم.

يمكن للوسيط وضع متطلبات المراقبة والأمن في السّحابة أو في مباني العميل. هذا يأخذ جزءاً من عبء الأمان خارج مزود السّحابة، الذي لا يملك عادةً الوقت ولا الموارد لمعالجة جميع المخاوف الأمنية للعملاء.

بدأت مؤخراً شركة Accenture الدولية للإستشارات وتكييف أنظمة تكنولوجيا المعلومات في العمل كوسيط سحابة ومزود لشركة تأمين كبيرة، وحسب Andrew Greenway قائد البرنامج العالمي للسّحابة في هذه الشّركة: "يتعرض عملاؤنا لضغوط هائلة للاستجابة لمتطلبات العمل للحصول على سرعة أعلى، يمكن للخدمات السّحابية تلبيتها بشكل جيّد، ولكن يجب إدارة التحدّيات مع الأمان والتكامل بعناية، وهذا هو المكان الذي يمكن للوسيط أن يضيف قيمة عليها."[37]

ثانياً: الطبيعة القانونية للسمسرة السّحابية

عند إنشاء شركة في لبنان تتعاطى التوسط السّحابي، أي وصف قانوني ينطبق عليها؟ هل هو وكيل للمزود، وسيط أم سمسار كما يدل اسمه "سمسار السّحابة"؟ أي عند حدوث أية مشكلة ما بين العميل والوسيط، بناءً على أي وصف قانوني تتم المحاسبة؟

أ. سمسار

عرّفت المادة 291 من القانون التجاري اللّبناني السّمسرة بأنّها عقد يلتزم فريق يدعى السّمسار أن يرشد الفريق الآخر إلى واسطة لعقد اتفاق ما أو أن يكون هو وسيطاً له في مفاوضات التعاقد وذلك مقابل أجر. فالسّمسار يقتصر دوره على إرشاد الطرف الآخر إلى فرصة التعاقد أو الواسطة في مفاوضات التعاقد، أي التقريب بين طرفي العقد ولا يتدخل مطلقاً لا في إبرام العقد أو في تنفيذه فهو لا يمثل عميله في الصّفقة. بمعنى آخر، إن السّمسار لا يبرم عقداً عن الطرفين أو عن أحدهما، وإنّما ينحصر دوره في التقريب بينهما وحملهما على التعاقد. ومتى أبرم الطرفان العقد انتهى دور السّمسار واستحق عمولة.

[36] **Gartner Inc.**: شركة استشارية وبحثية أمريكية في مجال التقنيات المتقدمة، يقع مكتبها الرئيسي في Connecticut Stamford.

[37] Supra 33.

أمّا الالتزامات التي تتولد عن هذا العقد الذي أبرمه الطرفان، فإنما تتولد في ذمتهما مباشرة، ولا يلتزم السّمسار بحسب الأصل بتنفيذ أو بضمان تنفيذ هذه الالتزامات، بل إنه يستحق عمولة حتى ولو لم يتم تنفيذ هذه الالتزامات ما دام العقد قد أبرم نتيجة لواسطة.
فالسّمسرة هي من عقود الوساطة التجارية التي تُبنى على أساس التوسط بين الأفراد الطبيعيين أو المعنويين، تجاراً كانوا أو غير تجار، وعمل السّمسار يقتصر على التوسط الذي هو عمل مادي صرف وليس له طابع قانوني.[38]
وبالتالي، فبالإمكان تطبيق وصف السّمسار على وسيط السّحابة، فكما سبق وذكرنا مهمته تبسيط العلاقة ما بين الطرفين، فهو يجمع الخدمات المتوفرة والبيانات التي يراد تطبيق هذه الخدمات عليها، ثم يطابق بين البيانات ونوع الخدمة الملائمة لها، ولكنه لا يبرم العقد نيابة عن العميل وإلّا أصبح وكيلاً وليس مجرد سمسار. فهل من المستطاع أن يكون وكيلاً؟

ب. وكيل

إن الوكالة كما عرّفتها المادة 769 من قانون الموجبات والعقود هي عقد بمقتضاه يفوض الموكل إلى الوكيل القيام بقضية أو بعدة قضايا، أو بإتمام عمل أو فعل أو جملة أعمال وأفعال، ويشترط قبول الوكيل. ويمكن أن يكون عمل الوكيل مادياً تبعاً للأعمال القانونية التي وكل بها.

وإذا كان يستنتج من تعريف الوكالة أن الإنابة من جوهرها إلّا أنه في بعض الحالات يعمل الوكيل باسمه الخاص دون إظهار إسم الموكل ولذا تكون الوكالة دون إنابة فلا تنشأ عنها علاقة مباشرة بين الموكل والغير[39]، ففي هذه الحالة لا تطبق قواعد الوكالة إلّا بين الموكل والوكيل فقط كما في حالة الوسيط التجاري أي الوكالة التجارية[40] التي نُصَّ عنها في المادة 272 من قانون التجارة اللّبناني: "تكون الوكالة تجارية عندما تختص بمعاملات تجارية. وبوجه أخص يسمى هذا العقد عقد وساطة ويكون خاضعاً لأحكام الفصل الآتي عندما يجب على الوكيل أن يعمل باسمه الخاص أو تحت عنوان تجاري لحساب من وكله. وعندما يجب على الوكيل أن يعمل باسم موكله تكون حقوقه وموجباته خاضعة لأحكام الكتاب الثاني من قانون الموجبات."

---

[38] جورج الأحمر، **العقود المدنية والتجارية**، محاضرات في الجامعة اللّبنانية كلية الحقوق والعلوم السّياسية والإدارية الفرع الثاني، خريف 2016–2017، ص. 51.

[39] المادة 799 من قانون الموجبات والعقود اللّبناني:"إذا عاقد الوكيل باسمه وبالأصالة عن نفسه، كانت له الحقوق الناشئة عن العقد، ويبقى مرتبطاً مباشرة تجاه الذي عاقدهم كما لوكان العمل يهمه وحده دون الموكل وإن يكن الذي عاقدهم قد عرفوه شخصاً مستعاراً أو وسيطاً يشتغل بالعمالة (العمولة)".

[40] علي مصباح ابراهيم، **العقود المسماة (البيع–الايجار–الوكالة)**، دار النشر مجهول، الطبعة الثالثة، 2012، ص. 425، 426، 432.

قد يحدث أحياناً أن يطلب العميل من وكيل الإشتراك بخدمة الحوسبة السّحابية بالإنابة عنه أو حتى أحياناً بدون الإنابة أي باسمه الخاص وذلك لعدّة أسباب ومن ضمنها عدم اضطلاع العميل/الموكل بتقنية خدمة السّحابة. فلا يكون لديه الخبرة اللّازمة في كيفية إدارة العلاقة التي تربطه بالمزوّد، يكون مفتقراً للخبرة والثقافة السّحابية، فيهتم الوكيل بالأعمال القانونية إضافةً إلى الأعمال المادية مثلاً كما الحال مع علاقة العميل بشركات الـ IT، ويمكن أن يكون وكيلاً للطرفين فيجمع الخدمات ويعيد بيعها.

مثلاً في لبنان يمكننا ذكر شركة NavLink [41] وشركة Zero and One[42] اللّتين هما وسيطتان سحابيتان، وهدفهما تثقيف المستخدم عن كل تطور تكنولوجي يسهل حياته ومساعدته على ايجاد المزوّد المناسب لمطالبه كذلك مساعدته على تنظيم عمله ليصبح بإمكانه الإستفادة القصوى من خدمة السّحابة.

سواء كان الشخص ينطبق عليه وصف السّمسار أو الوسيط التجاري أو الوكيل، يجب إثبات صفته من قبل الطرف المتضرر، وفي جميع الأحوال وبحسب الفقرة الثانية من المادة 291 من قانون التجارة، فقواعد الوكالة تطبق بوجه عام على السّمسرة؛ وبالتالي ينفتح السّوق اللّبناني على السّوق العالمي ويدخل مردود إلى الوكلاء بدون أن يتكلفوا بأية أعباء رأسمالية ويزوِّدوا المستخدمين بخدمات ظنّوا أن ليس باستطاعتهم الوصول إليها.

النبذة الثانية: طبيعة العلاقة بين المزود والعميل

سبق ورأينا أن العلاقة التي تربط بين المزود والعميل إمّا أن تكون مباشرة وإمّا أن تكون غير مباشرة أي بواسطة سمسار أو وكيل، فالعلاقة التي تربط بين العميل والوكيل أو السّمسار هي علاقة تعاقدية ترعاها قواعد عقد السّمسرة أو عقد الوكالة التي نصّ عليها في قانون التجارة وقانون الموجبات والعقود. أمّا العلاقة التي تربط السّمسار أو الوكيل مع المزود أو العميل عندما تقوم علاقته مباشرةً مع المزود، فهل هي علاقة تعاقدية أم غير تعاقدية؟ هل هذا العقد إذا ما كانت العلاقة تعاقدية هو عقد مسمى أم غير مسمى؟ هل هو عقد تراضي أم عقد موافقة (أي هو عقد إذعان أم عقد مساومة؟) هل هو عقد رسمي أم عقد رضى؟ عقد ذات عوض أم عقد مجاني؟

البند الأول: علاقة تعاقدية

بحسب ما سبق ذكره، إن مهمة الوكيل/السّمسار تكون أحياناً مفاوضة العقود عوضاً عن العميل، من هنا يمكننا استنتاج أن العلاقة بين المزود والعميل هي علاقة تعاقدية أي هناك عقد يربط ما بين الطرفين وينظم العلاقة أي واجبات وحقوق كل طرف. وغالباً ما يتم إبرام هذا العقد إلكترونياً عبر

---

[41] https://www.navlink.com/ (Accessed on August 30, 2018; at 09:20 AM)

42 https://www.zeroandone.me/ (Accessed on August 30, 2018; at 10:06 AM)

استعمال شبكة الانترنت، ونادراً ما نجد شركات لا تقدم إمكانية إبرام العقد على مواقع الويب الخاصة بها، فيتوجب على العملاء ابرام العقد خطياً بالطرق التقليدية أي باستخدام المستندات الورقية وبوجود الطرفين في مجلس واحد، ونرى هذه الحالة في الشّركة اللّبنانية Cirrus التي لا تزال تبرم عقودها بالطرق التقليدية فلا نجد على موقع الويب الخاص بها ما يدل على إمكانية لإبرامه إلكترونياً[43].

البند الثاني: علاقة إلكترونية

عقد الحوسبة هو غالباً عقد إلكتروني. وضع الفقه عدّة تعاريف لهذا العقد الأخير لا يختلف عن تعريف العقد بشكل عام مع مراعاة خصوصية كونه يعقد إلكترونياً.

عرّفه جانب من الفقه الفرنسي بأنه "اتفاق يتلاقى فيه الإيجاب والقبول بشأن الأموال والخدمات عبر شبكة دولية للإتصال عن بعد، وذلك بوسيلة مسموعة ومرئية تنتج التفاعل الحواري بين الموجب والقابل"[44].

أمّا الفقه الأميركي عرّفه بأنّه العقد الذي ينطوي على تبادل للرسائل بين البائع والمشتري تكون قائمة على صيغ معدة سلفاً ومعالجة إلكترونية، وتنشأ عنها إلتزامات تعاقدية[45].

لكن على الصّعيد التشريعي فنجد أن قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية للأمم المتحدة لم يتضمن تعريف مصطلح العقد الإلكتروني ولكنه إعتبر مصطلح "التعاقد الإلكتروني" إشارة إلى تكوين العقد عن طريق رسائل البيانات، وعرّف رسالة البيانات بـ "المعلومات التي يتم إنتاجها أو إرسالها أو استلامها أو تخزينها بوسائل إلكترونية أو بصرية أو بوسائل مماثلة، بما في ذلك على سبيل المثال لا الحصر تبادل البيانات الإلكترونية أو البريد الإلكتروني أو البرق، أو التلكس أو النسخ البرقي" كما وتضمنت الفقرة ب من نفس المادة (2) تعريف تبادل البيانات الإلكترونية حيث نصّت: يراد بمصطلح "تبادل البيانات الإلكترونية": نقل المعلومات إلكترونياً من حاسوب إلى آخر باستخدام معيار متفق عليه لتكوين المعلومات[46].

كما ويمكننا ذكر تعريف التعاقد عن بعد الذي ورد في المادة الثانية من التوجيه الأوروبي الصّادر في 20 أيار 1997 والمتعلق بحماية المستهلك في العقود المبرمة عن بعد بأنه "أي عقد متعلق بالسّلع

[43] www.itgholding.com/affiliate/4/cirrus (Accessed on August 30, 2018; at 12:12 PM).

[44] سمير حامد عبد العزيز الجمال، **التعاقد عبر تقنيات الاتصال الحديثة**، (رسالة دكتورا) جامعة القاهرة، 2005، ص. 66.

[45] الصّالحين أبو بكر العيش، **الشّكلية في عقود الإنترنت**، بحث منشور على الموقع:
http://www.lawoflibya.com/forum/showthread.php?t=2897

[46] قانون الأونسترال النموذجي بشأن التجارة الإلكترونية مع دليل التشريع، 1996.

والخدمات التي ينظمها المورد والذي يتم باستخدام واحدة أو أكثر من وسائل الإتصال الإلكترونية حتى إتمام التعاقد"[47].

البند الثالث: عقد غير مسمى

إن عقد الحوسبة السّحابية هو عقد غير مسمى أي أن المشرع اللّبناني لم يأتِ على ذكره بين النصوص التي نظمها في قوانينه ونظم قواعدها، فهو لم يخص هذا العقد بتسمية معينة ولم يعن بتنظيمها وإنما ترك أمر التنظيم للفرقاء، ووجود هذا النوع من العقود يرتبط بمبدأ الحرية التعاقدية من جهة وتطور الحياة الإقتصادية التي تؤدي إلى ظهور العديد من الحاجات الجديدة من جهة أخرى الأمر الذي يستدعي وجود صيغ تعاقدية جديدة باستمرار لمواجهتها[48] .

البند الرابع: عقد مختلط

يطرح السّؤال، هل هو عقد إذعان أم عقد مساومة أم عقد استهلاك؟
بما أن عقد السّحابة هو عقد إلكتروني، وبما أن الفقه انقسم في تحديد طبيعة العقد الإلكتروني إلى عدّة اتجاهات، فيمكننا اعتماد التقسيم ذاته على العقود السّحابية، فمنهم من رأى أنها عقود مساومة، ومنهم من رأى أنها عقود إذعان والإتجاه الثالث حددّ طبيعتها بحسب الطريقة المستعملة لإبرام العقد:

الاتجاه الأول: إنها عقود مساومة

يرى أنصار هذا الإتجاه أن العقود الإلكترونية هي عقود مساومة وليست عقود إذعان، لأن حرية العميل غير مقيدة بمجرد الموافقة أو الرفض على شروط العقد الذي ينفرد بوضعها المزود، لكنه لديه الحرية بالتعاقد مع أي مقدم خدمة آخر إذا لم تناسبه الشروط التي تظهر في عقود هذا المزود، فيمكنه الانتقال إلى مزود آخر إذا ما كانت شروطه أفضل أو تناسبه أكثر. إذاً لا ينطبق عليها الشّروط التي تميّز عقد الإذعان ولكن يجدون أن مبدأ الرضائية هو السّائد[49].

---

[47] التوجيه الإوروبي الصّادر في 20 أيار 1997 والمتعلق بحماية المستهلك في العقود المبرمة عن بعد.

[48] إيلي داغر، **محاضرات في القانون المدني**، الجامعة اللّبنانية كليّة الحقوق والعلوم السّياسية والإدارية، الفرع الثاني.

[49] رمزي بيدالله علي الحجازي، **الحماية المدنية للمستهلك بعد التعاقد الإلكتروني**، منشورات الحلبي الحقوقية، بيروت، 2016، ص. 43.

الاتجاه الثاني: إنها عقود إذعان

يستند أنصار هذا الرأي إلى حقائق موضوعية، وهي أن المهني في مركز اقتصادي ومعلوماتي قوي، وأن العقد يتعلق بسلع وخدمات لا غنى عنها للمستهلك الذي يسعى لتلبية حاجاته الشّخصية أو حاجات عمله بالإضافة إلى أن الإيجاب يعد عاماً موجهاً لجمهور غير محدد، ولوقت غير محدد، وتتم صياغة شروطه في قالب نموذجي تتسم الصّياغة فيه بالتطرق لمسائل فنية دقيقة كعنوان للعلاقات العقدية الحديثة التي تفتقر إلى الوضوح، وإن كانت واضحة فلا يتسيّر فهمها للشخص العادي، وحيث أن الشخص/المستهلك يذعن للإيجاب الإلكتروني بما يتضمنه من شروط مطبوعة، فلا يملك احتمالية تعديلها مما يوجد اختلالاً عقدياً بين طرفي العقد[50] .

الإتجاه الثالث: إنها عقود تحدد طبيعتها بحسب الوسيلة المستخدمة في التعاقد

يرى أنصار هذا الإتجاه بأن العقد الإلكتروني (قياساً للعقد السّحابي) قد يكون رضائياً، وقد يكون إذعاناً وذلك يتوقف على الوسيلة المستخدمة في إبرامه.

فقد يتاح للمتعاقد العميل التفاوض بحرية حول شروط العقد وتبادل وجهات النظر مع الطرف الآخر (المزود)، والفصل بين العروض المطروحة في حال كان التعاقد يتم بوسيلة تتيح ذلك، فيكون العقد في هذه الحالة عقداً رضائياً ويعد العقد والحالة هذه من قبيل عقود المساومة.

أمّا إذا تمّ التعاقد عبر مواقع الويب التي تستخدم النماذج الإلكترونية التي تكون شروطها معدّة سلفاً بحيث لا يجد المستهلك معها مجالاً للمناقشة والمفاوضة في هذه الشروط فيكون في هذه الحالة الطرف الأضعف في العلاقة العقدية، ويكون بالتالي عقد إذعان[51].

فيمكن اعتماد الاتجاه الثالث في عقود الحوسبة السّحابية، إذ إن هناك عدّة أنواع سحابات، فمنها خاصة ومنها عامة ومنها مختلطة وفي كل منها تختلف طريقة التعاقد كما سنرى لاحقاً في الدراسة، كذلك تختلف طريقة التعاقد من مستهلك شخصي ومن متعاقد محترف. ولكن غالباً تكون العقود التي تبرم بين المحترف مقدم الخدمة والجمهور عقود إذعان أمّا تلك التي تكون بين محترفين يمكن المفاوضة على تفاصيل العقد بينهما فتكون عقود مساومة. وبالتالي عند دراسة العقد يجب تفريق صفة كل من الطرفين، فعند وجود تفاوت في الصّفات يجب النظر إلى العقد على أنه عقد استهلاك لكي يتمتع الجمهور بالحماية.

---

[50] أسامة بدر، **حماية المستهلك في التعاقد الإلكتروني**، دراسة مقارنة، دار الجامعة الجديدة للنشر، الإسكندرية، 2005، ص. 191-192.

[51] رمزي بيدالله علي الحجاوي، **مرجع سابق**، ص. 44-45.

البند الخامس: عقد معاوضة

إنه من عقود المعاوضة سواء أكان بمقابل نقدي مباشر من العميل عبر بطاقات الدفع الالكتروني أو لا. ففي بعض العقود النموذجية والخدمات، يكون الإشتراك في الخدمة بشكل مجاني فيشترك الشخص بالخدمة بنقرة واحدة، فيعتقد أنه يستفيد من الخدمة مجاناً، ولكن ما النفع الذي يحصل عليه مزود الخدمة لقاء تأمينه للخدمة بشكل مجاني؟ ألا يمكن أن يكون مقابله بيانات العميل التي يحفظها على السّحابة؟ هل يتصرف المزوّد بهذه البيانات؟ هل يقوم ببيعها لشركات أخرى؟ سنتناول أيضاً كافة هذه النقاط في الفصول القادمة.

إستخلاصاً مما سبق ذكره، يمكن تعريف الحوسبة السّحابية بأنها عقد غير مسمى في القانون اللّبناني يبرم بين مزوِّد الخدمة والمستخدم بالطرق الإلكترونية، يكون تارةً عقد إذعان إذا أبرم مع مستهلك ضعيف وتارةً أخرى عقد مساومة إذا أبرم مع طرف قوي، فيقدم المزوّد بموجب هذا العقد خدمة مقابل عوض يتم مقاضاته من المستخدم بطريقة مباشرة أم غير مباشرة.

المبحث الثاني: تمايز الحوسبة السّحابية

دخلت الحوسبة السّحابية حياة كل شخص طبيعي ومعنوي وحكومي، ويتداخل مفهومها أحياناً بغيرها من المفاهيم التقنية أو تكمل بعضها البعض، فوجود تقنيات جديدة سببه التطور التكنولوجي المتواصل فإذا ما نشأت تقنية حديثة كانت لتطوير تقنية سابقة أو تلبيةً لحاجات جديدة، فما هي تلك التقنيات التي يتداخل مفهومها بمفهوم السّحابة؟ كذلك فكرة السّحابة كونها تقديم خدمة وكونها عقداً قد يتداخل مع غيره من المفاهيم القانونية كعقد الإيجار وغيره، فبمَ يتميّز عقد السّحابة عن العقود التي قد تتلابس معه؟

الفقرة الأولى: تفريق الحوسبة السّحابية عن غيرها من المصطلحات التقنية

الحوسبة السّحابية مصطلحٌ جديد ولكن هناك مصطلحات أجد وأكثر تعقيداً نسمعها كل يوم، قد نظن أنها تدخل في مفهوم السّحابة، فمنها ما هو واضح أن له علاقة بها ولا يتطلب البحث مفصّلاً ولكن يجب ذكره فقط كالـ Datacenters أي مركز البيانات التي هي عبارة عن بنية تحتية وعملية فنية مخصصة لاستضافة تركيز كبير من أجهزة الكمبيوتر تكون مؤمنة وعلى اتصال دائم بالطاقة الكهربائية

والتبريد للآلات... وبالتالي هي المركز حيث تقدم خدمة السّحابة ولكن يمكن للبعض إنشاء مركز بياناتهم الخاص[52].

لكن هناك مصطلحات أحدث يجب إظهار علاقتها بالسّحابة إذا ما وجدت كالـ virtualization والـ Big Data والـ Blockchain.

النبذة الأولى: التمثيل الإفتراضي La virtualization

كلمة virtual تعني ظاهري أو وهمي، والـvirtualization هي عملية صنع نسخة وهمية وليست حقيقية من شيء ما، مثل نظام التشغيل أو السّيرفر server أو وحدة التخزين storage device أو أحد موارد الشّبكة Network Resource [53].

وقد يعتقد البعض أن هذه التقنية حديثة العهد، لكن في الحقيقة ظهرت في عام 1960 للمرة الأولى وأول من طوّرها كانت شركة IBM أو International Business Machines في كامبرج ماساتشوستس، إذ إن أجهزة الكمبيوتر في ذلك العصر وأخص بالذكر جهاز (IBM 7044 M44) الذي كان يقوم بعملية معالجة واحدة كل مرّة والذي انعكس سلباً على مقدرة المعالجات للعمل وخصوصاً أن تطوير قوة المعالجات لم يكن بالأمر الصّعب فكانت سبباً في ولادة تقنية التمثيل الإفتراضي التي أتاحت استخدام قوّة المعالج من قبل عدّة أشخاص من خلال تقسيمه إلى عدّة أجهزة وهمية يتم التحكم بها بأجهزة مخصصة أو Client وبالتالي أتاح لهم إمكانية تشغيل أكثر من تطبيق واحد في الوقت نفسه.[54]

فهي عملية خلق نظام تشغيلي وهمي تستخدم برنامجاً متخصصاً للقيام بتشغيل أكثر من نظام تشغيل على نفس الجهاز Hardware في الوقت نفسه، فهدفها فصل نظام التشغيل عن الـ Hardware الذي يعمل عليه، بحيث يصبح النظام التشغيلي يعمل في بيئة تخيلية كأنها حاسوب منفصل. هذه التقنية تتيح مشاركة الموارد الحقيقية وتشغيل أكثر من نظام تشغيل على نفس الموارد في اللّحظة ذاتها.

---

[52] Guide sur le Cloud Computing et les Data Centers, à l'attention de collectivités locales, sous la surveillance du ministère de l'économie de l'industrie et du numérique française, juillet 2015, p. 17.

[53] محمد عمر، **ماهي تكنولوجيا الـ Virtualization**، 6 تشرين الثاني 2014، منشور على networks4ar.blogspot.com. (http://networks4ar.blogspot.com/2014/06/virtualization.html) (Accessed on 8 August 2018 at 12:21 PM).

[54] Jim Sweeney, Virtualization: An Overview, published in **Encyclopedia of Cloud Computing**, John Wiley & Sons Ltd., United Kingdom, 2016, p.90.

بالرغم من اختلاط مفهومي الحوسبة السّحابية والتمثيل الإفتراضي في معتقد البعض إلّا أنهما مختلفان ولكن هناك علاقة بين الإثنين، فالتمثيل الإفتراضي هو العنصر الأساسي في الحوسبة السّحابية وتساعد في جعلها ذات قيمة للمستخدمين.

نظراً لأن الـ virtualization هي أحد مكونات الـ cloud[55]، فالمسألة ليست مسألة اختيار، فكلاهما يجعلان من الممكن تقليل موارد الكمبيوتر والتكاليف وزيادة فعالية الشّركة. وبالرغم من ذلك، لا يمكن اعتبارهما مرادفين، بينما التمثيل الإفتراضي تقنية لمحاكاة العديد من الحالات الإفتراضية من خلال نفس الجهاز المادي، فالسّحابة تجعل من السّهل تنظيم وإدارة هذه الحالات الإفتراضية وتقدمهم عن طريق خدمة مدفوعة الأجر.

وبالتالي لا تعد الـvirtualization جوهر مفهوم السّحابة، ولكن بالنظر إلى التقدم التكنولوجي الحالي في إدارة البنية التحتية لتكنولوجيا المعلومات، فأنها الآن جزء لا يتجزأ من عمليتها. ومن هذا المنطلق يجب فهم التكامل بين هذين المفهومين[56].

النبذة الثانية: البيانات الكبيرة Big Data

بعد السّحابة، ظهر مصطلح "Big Data" الإنكليزي أي البيانات الكبيرة أو الضخمة، والتي هي في اللّغة الفرنسية "grosse donnée" أو "données massives"، جاءت تعبيراً من الولايات المتحدة وتشير إلى مجموعة البيانات الكبيرة جداً لتنفيذ أدوات إدارة محددة. فماهي البيانات الكبيرة؟

إقترح Butler عام 2013[57] تعريفاً لها على أنها بيانات نمت إلى حجم يتطلب تقنيات جديدة لتخزينها وتنظيمها وتحليلها. هذا تعريف مقبول مؤقتاً إلّا أن خبراء البيانات سيجدون طرقاً لمعالجة ما هو معروف بالـBig Data.

---

[55] Kapil Bakshi and Craig Hill: "Cloud Network and I/O Virtualization", published in **Encyclopedia of Cloud Computing**, John Wiley & Sons Ltd., United Kingdom, 2016, p. 102.

[56] Ivision: "**Cloud et Virtualisation: les differences**", publié sur: ivision.fr. (Valide sur: https://www.ivision.fr/cloud-et-virtualisation-les-differences/) (Consulté le 8 Aout 2018 à 10:05 AM).

[57] Butler B (2013): **Amazon Web Services Worldwide Public Sector Summit**, Washington DC, September 10, 2013. (Available on: http://d36cz9buwru1tt.cloudfront.net/145AB-EMR-for-Fun-and-Profit-final.pdf) (Accessed on August 6, 2018 at 13:00PM).

تعد الـ Big Data مسألة استراتيجية جديدة للشركات وللدول. قرر البيت الأبيض تخصيص 200 مليون دولار لإنشاء الأدوات التي تحلل كميات كبيرة جداً من البيانات من أجل تحسين البحث العلمي في الولايات المتحدة. فالإدارة الأمريكية تريد استغلالاً أفضل لقواعد بياناتها الكبيرة كما وتدريب الباحثين للحصول على أكبر قدر من الفائدة من البحث العلمي والبيئة والطب الحيوي وبالطبع للأمن القومي. بدأت أوروبا أيضاً في إدراك أهمية هذا التحدي وجزء من برنامجها للإستثمارات في المستقبل، كما وأطلقت فرنسا دعوة للمشاريع على البيانات الكبيرة حيث سيتم تخصيص ميزانية لها وقدرها 25 مليون يورو. الغرض من هذا النهج هو المساعدة في التغلب على بعض الحواجز التكنولوجية التي تحول دون هندسة الأدوات التي تتعامل مع كميات كبيرة من البيانات وأنظمة التشغيل المناسبة[58].

تتمثل الإشكالية الأولى للدول كما للشركات، في جمع وتخزين هذه الكميات الكبيرة من البيانات والمعلومات، وهذا يتطلب استخدام وسائل حوسبة ونسخ احتياطية مهمة يمكن أن تنمو بسهولة وبسرعة عند الطلب لاسيما من استضافة البيانات والطاقة الحاسوبية. من هذه الاشكالية يمكن استحضار مفهوم الحوسبة السّحابية التي سبق وأشرنا إلى مزاياها، فالـ Big Data يمكن وضعها على الـ Cloud كما وتحليل هذه البيانات يمكن أن يتم على السّحابة[59].

البنوك هي مثال على من لديه بيانات ضخمة، فمع تدفق الكميات الكبيرة من المعلومات من مصادر لا تعد ولا تحصى، تواجه البنوك مشكلة إيجاد طرق جديدة ومبتكرة لإدارة وحفظ البيانات الضخمة. في حين أنه من المهم فهم العملاء وتعزيز رضاهم، وتقليل المخاطر والاحتيال إلى الحد الأدنى مع الحفاظ على الامتثال التنظيمي. تجلب البيانات الضخمة رؤى كبيرة، ولكنها تتطلب أيضاً أن تظل المؤسسات المالية متقدمة على اللّعبة بتحليلات متقدمة[60].

بالخلاصة، يمكن القول إن الانتقال الى السّحابة فيما خص الـ Big Data، تمكن الشركات من الحصول على فرصة لتبسيط أداة النسخ الاحتياطي عن طريق تبسيط العملية ومركزيتها فيستفيدون من فوائد البنية التحتية الإفتراضية.

---

[58] Cogeco Peer 1: "**Le Big Data: un nouveau défi pour l'hébergement en cloud et la sauvegarde des données**", 12 avril 2012. (Valide sur: https://www.cogecopeer1.com/fr/le-big-data-un-nouveau-defi-pour-lhebergement-en-cloud-et-la-sauvegarde-des-donnees/) (Consulté le 6 Aout 2018 à 10:12 AM).

[59] Mark Smiley: "**Big Data in a cloud**", published in **Encyclopedia of Cloud Computing**, John Wiley & Sons Ltd., United Kingdom, 2016, p. 554

[60] https://www.sas.com/en_us/insights/big-data/what-is-big-data.html. (Accessed on August 9, 2018 at 09:21 AM).

النبذة الثالثة: تقنية البلوك تشين Blockchain

مع تسارع التطور التكنولوجي، نسمع دائماً بمصطلحات جديدة قد يصعب على الكثيرين فهمها، فمؤخراً أي شخص كان يتابع الاتجاهات في التكنولوجيا والتمويل، قد سمع بالـ Bitcoins التي تدار من خلال الـBlockchains. وقد تساءل عمّا إذا كان هذا الـ Blockchain سيكون بعد الحوسبة السّحابية أو الـBig Data أو حتى انترنت الأشياء (IoT)[61].

الـ Blockchain والمعروف أيضاً بـ distributed ledger أي دفتر الأستاذ هي التكنولوجيا التي تعمل لبدء معاملات bitcoin، فهي قاعدة البيانات المؤمنة التي تسجل هذه البيانات.

عرّفها Leighton Cosseboon في مقاله المنشور على Techinasia.com:

"A blockchain is nothing more than a record of online events. The ledger is public, and shared among all different parties on a network-node on the blockchain. It can only be updated by consensus from a majority of the users in the system. Additionally, once entered, the history is permanent and can never be deleted; ever… a blockchain is a highly-distributed, leaderless, jurisdictionless, identityless, nearly anonymous, decentralized architecture for managing ownership."[62]

أي أنها ليست أكثر من سجل بيانات للأحداث عبر الإنترنت، فهذا السّجل هو عام ومشترك بين جميع الأطراف المختلفة على شبكة الـ Blockchain، لا يمكن تحديثه سوى بتوافق آراء غالبية المستخدمين. إضافةً إلى ذلك، فبمجرد الدخول يسجل على اللّائحة ولا يمكن حذفه على الإطلاق. فالـ Blockchain هو بنية عالية التوزيع، بلا قيادة، بلا سلطة، مجهولة الهوية تقريباً ولا مركزية لإدارة الملكية.

من التعريف السّابق يمكننا الاستنتاج أنها تسمح للأطراف المتعددة التي لا تثق بعضها ببعض لمشاركة المعلومات دون الحاجة إلى مسؤول مركزي. تتم معالجة المعاملات بواسطة شبكة من

---

[61] إن مصطلح IoT: Internet of Things يستخدم إلى وصف العلاقة بين الكائنات، فالتقدم التكنولوجي جعل من الممكن للأشياء التي لم يكن من المستطاع أن تتواصل في الماضي أن تقيم علاقة ذت مغزى اليوم. فمثلاً إذا انكسر جهاز تحكم التلفاز، لم يكن من المستطاع تشغيل التلفاز في الماضي من دونه ولكن اليوم فيمكن استخدام الهاتف كجهاز حكم وهذه هي قوة انترنت الأشياء التي جعلت ذلك ممكناً عن طريق التكنولوجيا.

[62] MURFETT LEGAL: "**Blockchains- "The Most Important Invention Since The Internet Itself**", 2017.

(Available at: https://www.murfett.com.au/Murfettlegal/media/Documents/Article/35-Blockchains-The-Most-Important-Invention-Since-The-Internet-Itself.pdf) (Accessed on August 9, 2018 at 14:14 PM).

المستخدمين تعمل كآلية توافق في الآراء بحيث يقوم الجميع بإنشاء نفس نظام السّجل المشترك في الوقت نفسه. قيمة هذه الرقابة غير المركزية هي أنها تقضي على مخاطر السّيطرة المركزية. عند استخدام قاعدة بيانات مركزية، يمكن لأي شخص لديه إمكانية وصول كافية إلى هذا النظام تدمير البيانات أو إفسادها. وهذا يجعل المستخدمين يعتمدون على المسؤولين الذين يحظى بعضهم بثقة المستخدمين، ففي بعض البنوك مثلاً لم تحصل أية عملية سرقة عند حفظها في private databases، ولكن تلك الثقة تكلف البنوك بلايين الدولارات للحفاظ على هذه الـ databases وحمايتها من أية اختراقات، وعند حدوث أيّ اختراق تكون خسارة للمستخدم. كذلك بالنسبة لتسجيل البيانات، فبإمكانها الإحتفاظ بالمعلومات ذات الصّلة عند حدوثها وأيضاً بجميع المعلومات التي سبقت. إنها تنمو كمحفوظات آخذة في التوسع من بياناتها المسجلة مع توفير صورة في الوقت الحقيقي تمكننا من رؤية تطور قاعدة البيانات إلى نظام قياسي recording system.

بالنسبة للثقة والسّرية، إذا كانت السّرية هي الهدف الوحيد والثقة ليست قضية، فإن قاعدة بيانات blockchain لا تشكل أي ميزة على قاعدة البيانات المركزية. إذ إنه يتطلب لإخفاء المعلومات عليها الكثير من التشفير وعبء حسابي متعلق بالعقد في الشّبكة. لا توجد طريقة أكثر فعالية من إخفاء البيانات بالكامل في قاعدة بيانات خاصة لا تتطلب حتى الاتصال بالشبكة[63]. فالـ Blockchain ليست حوسبة سحابية كما عرّفناها في هذه الدراسة، إنما هي تقنية تتعلق فقط بالتحاويل المالية، كما وأنها ليس لديها مركز بيانات فهي لديها نفس طبيعة مكينة الفاكس كما وصفها Lary Summers وزير الخزانة الأمريكية سابقاً[64].

أليس من الممكن جمع هاتين التقنيتين بتقنية واحدة يمكن تسميتها مثلاً بالـ Blockcloud؟

من حيث المبدأ، يمكن تصور مثل هذا النظام بسهولة. كل ما يحدث للبيانات من نقل أو معالجة أو تخزين لها يتم إدخاله إلى الـ blockchain.

يمكن التحقق من أي شخص له حق الوصول إلى البيانات ويراقب عمله ويحدد وقت دخوله على البيانات وإحداثه أي تغيير أو تعديل مهما كان بسيطاً وذلك بالوقت الحقيقي وعليه يمكن مساءلة المسؤول عن التعديل.

[63] Nolan Bauerle: "**What is the difference between a blockchain and a database?**" (Available on: https://www.coindesk.com/information/what-is-the-difference-blockchain-and-database) (Accessed on August 9, 2018 at 15:11 PM).

[64] Ian Khan: "**What is Blockchain Technology? A Step-by-Step Guide For Beginners**, March 1, 2019, published on: blockgeeks.com. (https://blockgeeks.com/guides/what-is-blockchain-technology/) (Accessed on August 9, 2018 at 13:29 PM).

لكن هل يمكن إنشاء مثل هذا النظام حقيقةً؟[65]

الفقرة الثانية: تفريق الحوسبة السّحابية عن غيرها من العقود

الحوسبة السّحابية تنشئ علاقة تعاقدية بين طرفيها كما رأينا سابقاً، وعقد هذه الخدمة السّحابية هو عقد غير مسمى في القانون اللّبناني فلم يكن موضع دراسة من قبل المشرع، بالرغم من وجود عقد يحكم إرادة المتعاقدين، لكن إلى أي عقد منصوص عليه في القانون اللّبناني يمكن مقاربته؟

النبذة الأولى: عقد الحوسبة السّحابية وعقد الوديعة

قد يشبّه البعض عقد الحوسبة السّحابية بعقد الوديعة لأن غرضه الأساسي هو حفظ الأشياء المودعة وصيانتها[66]. ويقوم عقد الحوسبة على نقل البيانات إلى مزوّد الخدمة الذي يقع عليه موجب الحفاظ عليها في الخوادم. إلّا أنه لا يمكن إعتبار عقد الحوسبة عقد إيداع منظم، إذ إن المزوّد قد لا يعرف ما إذا كانت المساحة المستخدمة محتوية على بيانات أو أنها خالية منها. ففي عقد الوديعة عليه أن يستلم الوديعة التي هي شيءٌ منقولٌ حسب المادة 690 من قانون الموجبات والعقود.

فالعقد يتضمن في الحقيقة بعض من أحكام عقد الوديعة، فعند استلام الوديعة لا يحق للوديع أن يستعملها بدون إذن المودع[67]؛ كذلك في ما يتعلق بالسّحابة لا يحق للمزوّد أن يستخدم البيانات التي تحفظ لديه إلّا إذا سمح له المستخدم بذلك إلّا أن واقع الحال مختلف عن ذلك كما سنرى لاحقاً. فالإلتزام بالحفظ هو جوهر عقد الوديعة. كما يلتزم برد الوديعة عند نهاية العقد، كما هو الحال في عقد السّحابة، إلّا إن في هذا الأخير قد يبقى لدى المزوّد نسخة عن البيانات وبالتالي لا يكون موجب الرّد قد تحقق.

كما واستلام الوديعة يختلف عن نقل البيانات، فإستلام الوديع لها يكون مادياً أي أنه يستلم شيئاً مادياً ملموساً، أمّا المزوّد فيستلم شيئاً غير مادي. المستخدم في عقد السّحابة قد يترك المساحة العائدة له من الخادم فارغة فلا يتم موجب التسليم والإستلام بالرغم من الإبقاء على موجب صيانة الخادم من قبل المزوّد.

وبالتالي لا يعتبر عقد السّحابة عقد وديعة بالرغم من التلاقي بين العقدين في موجب الحفاظ على الأشياء المودعة لدى الطرف الثاني.

---

[65] Mike Gault: "**BlockCloud: Re-inventing Cloud With Blockchains**", May 13, 2018, published on: www.guardtime.com. (https://www.guardtime.com/blog/blockcloud-re-inventing-cloud-with-blockchains) (Accessed on August 9, 2018 at 16:52 PM).

[66] المادة 690 من قانون الموجبات والعقود.

[67] المادة 700 من قانون الموجبات والعقود.

النبذة الثانية: عقد الحوسبة السّحابية وعقد الإيجار

إن عقد الإيجار أو إيجار الأشياء هو عقد يلتزم بموجبه المؤجر بأن يولي المستأجر حق الإنتفاع بشيء ثابت أو منقول لمدة معينة مقابل بدل يلتزم المستأجر بتأديته له[68]. أمّا الموجبات الأساسية التي تقع على عاتق المؤجر فهي تسليم المأجور وصيانته والضمان.

فهل يدخل عقد السّحابة في مفهوم هذا العقد؟

مما لا شك به أن هناك موجبات مشتركة بين العقدين، منها وضع المزوّد مساحة من الخادم تحت تصرف المستأجر أو المستخدم من أجل الإنتفاع بها بحرّية تامة من دون أن يكون له حق الإطلاع على الأشياء المحفوظة في داخلها، بل يبقى للمستأجر وحده معرفة ما هي البيانات الموجودة في داخلها. وقد يترك المساحة فارغة دون أن يؤثر ذلك على عقد الإيجار.

بالفعل هناك تشابه بين هذين العقدين لجهة إلتزام المزوّد بتمكين العميل من الإنتفاع خلال مدة معينة بالمساحة في الخادم عن طريق تمكينه إلكترونياً بالحصول على مفتاح للإستفادة من هذه المساحة وهذا المفتاح عبارة عن account and password. كما يلتزم بالصّيانة أي صيانة الخادم وضمان العيوب، في مقابل إلتزام العميل بأداء البدل المتفق عليه إذا ما وجد. كذلك يحق للمستخدم الدخول بطريقة إلكترونية بالطبع إلى مكان تواجد البيانات والحصول عليها وإستخدامها دون إذن مسبق من قبل المزوّد.

هذا العقد يتنافى مع عقد الإيجار بأن المزوّد ملتزم بالسّهر على الخوادم والحفاظ عليها إذ إن في عقد الإيجار تنتقل حيازة الشّيء المؤجر إلى المستأجر فيتولى السّهر عليها بنفسه. كما إنه لا يمكن الجزم بما إذا كان إيجاراً منقولاً أو غير منقول أو نوع إيجار جديد غير منصوص عليه في القانون، إذ إن الشّيء المؤجر هو مساحة في شيء منقول (الخادم) والمساحة هي شيء إفتراضي.

ومن هنا نلاحظ أن عقد الإيجار لا ينطبق تماماً على عقد السّحابة وإن كان هناك نقاط كثيرة مشتركة. لكن على المشرّع والقضاء الجزم وأخذ موقف والإجتهاد أكثر في هذه الأمور التقنية الحديثة كما فعل في ما يتعلق بالصّناديق الحديدية في المصارف التي تتشابه بالمفهوم مع الحوسبة السّحابية بفارق واحد أن الأشياء المودعة في الصّناديق عادةً ما تكون مادية وتلك المحفوظة في السّحابة تكون غير مادية. فنصت المادة 309 من قانون التجارة اللّبناني على "إن الودائع التي توضع في الصّناديق الحديدية أو في خانات منها تطبق عليها قواعد إجارة الأشياء. ويكون المصرف مسؤولاً عن سلامة الصّناديق المأجورة"، كذلك القضاء اللّبناني إعتبر بمعظمه أن عقد إيجار الصناديق الحديدية هو عقد إيجار الأشياء[69].

---

[68] المادة 533 من قانون الموجبات والعقود.

[69] الياس ناصيف، **العقود المصرفية**، منشورات الحلبي الحقوقية، الطبعة الثانية، بيروت، 2012، ص. 115.

الفصل الثاني: كيفية إبرام عقد الحوسبة السّحابية

بعد أن فرّقنا عقد الحوسبة عن غيره من العقود وبعد أن بحثنا في الطبيعة القانونية لهذا العقد، يجب التطرق إلى كيفية إبرام العقد، ما هي حاجات المستخدم؟ ما هي أنواع وأنماط السّحابة التي هم بحاجة إليها؟ كذلك ما هي صفة المستخدم؟ إذ إن طريقة إبرام العقد تختلف بين مستهلك عادي وبين شركة وحكومة. فما هي أساليب إبرام هذا العقد؟ هل يمكن للمستخدم المفاوضة عليها أم هي عقود إذعان؟ مَن مِن هؤلاء المستخدمين بحاجة لحماية عند إبرامه العقد؟ وهل هناك من نصوص في القانون اللّبناني تحميه في ظل هذا التعاقد؟ هل هناك نقص في التشريع اللّبناني في هذا الإطار؟

المبحث الأول: توافرية خدمات الحوسبة السّحابية وفق حاجات ومتطلبات المستهلك

دخلت التكنولوجيا حياة جميع الأشخاص ويمكن تفريق الأشخاص بحسب نوعهم، فهناك أشخاص طبيعيين وأشخاص معنويين وأشخاص حكوميين، وكل طرف من هذه الأطراف يلعب دوراً مهماً أكان على صعيد الدولة، على الصّعيد الإجتماعي والإقتصادي وصولاً إلى الصّعيد الشّخصي، وعلى كل صعيد هناك متطلبات وإستخدامات تختلف بحسب طبيعة العمل وهناك عدّة نماذج وأنماط للسّحابة تؤمن هذه الإستخدامات وتسهل الطلب.

الفقرة الأولى: أنماط الحوسبة السّحابية التي يمكن الإشتراك بها

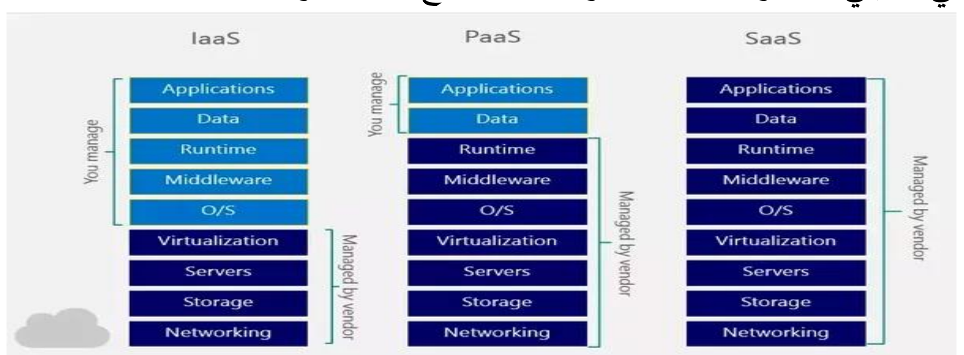
سنناقش أنماط الحوسبة السّحابية من أنواع ونماذج الخدمات المتوفرة فيها والتي تعد واحدة من أهم المفاهيم المتعلقة بالحوسبة السّحابية. الحوسبة السّحابية موجهة بالأخص نحو الأعمال والشّركات، فيتوجب على هذه الأخيرة معرفة طرق النشر في السّحابة وأية سحابة عليها اختيارها بحسب احتياجاتها، متطلباتها وميزانيتها والأمان الذي توفره. فالخيار غير الصّائب قد يؤثر على الشّركة بطريقة سلبية. فهناك عدد كبير من مستخدمي السّحابة ولكل مستخدم حاجات تختلف عن حاجات الآخر، فيقدم مزودو السّحابة الكثير من الأنواع والنماذج التي سنقوم بذكرها في هذه الفقرة.

النبذة الأولى: نماذج الحوسبة السّحابية

النماذج الأساسية للحوسبة السّحابية هي IaaS، PaaS وSaaS هي الأكثر استعمالاً والأكثر انتشاراً بين المستهلكين، واليوم أصبحت السّحابة التكنولوجيا المهيمنة التي تقود عالم تكنولوجيا المعلومات IT World. ومع تزايد حاجات المستهلكين، الكثير من مزودي الخدمة بدأوا بتأمين خدمات منفصلة تتطابق مع حاجات المستهلكين كالشّبكات، مراكز البيانات، التخزين وكلّها وفق طلب ووقت طلب المستهلك. فمن هذه الخدمات Network as a Service (NaaS)، Desktop as a

Database as a Service ،Storage as a Service (STaaS) ،Service (DEaaS) (DaaS)، Security as a Service (SECaaS)، وكلّ واحدة من هذه الخدمات تقدم الخدمة المذكورة في اسمها فمثلاً الـ SECaaS تقدم خدمة الأمان للمستخدمين عند طلبهم مثلاً الأمان في استخدام البطاقات المصرفية. كذلك كل خدمة تنتهي بـ "as a service" هي خدمة حوسبة سحابية.

أمّا في ما يلي سنتطرق ملخصاً لفكرة عمل للنماذج الثلاثة الرئيسية.



ولتبسيط الفرق بين هذه الخدمات، يمكننا اعتبار الحالات التالية،

إذا قام شخص ببيع جهاز كمبيوتر، يكون الشّاري متحكماً في البيانات التي يعالجها باستخدامه هذا الجهاز. فالبائع ليس معالجاً لأي من هذه البيانات حتى لو كان الكمبيوتر يحتوي على برنامج تم تحميله مسبقاً من قبل البائع أو طرف ثالث والذي يُستخدم لمعالجة البيانات، فلا يزال البائع غير معالج للبيانات إذ إنه فقط قام بتزويد الشّاري بالأجهزة والبرامج. حتى لو اتفق أن البائع يقوم بتحديث البرامج كلما وجدت مقابل رسوم.

كذلك، إذا أجر شخص جهاز كمبيوتر، واستخدمه المستأجر في المبنى الخاص به لمعالجة بياناته، فالمؤجر لا يعتبر معالجاً للبيانات حتى لو قام هو بتوفير الجهاز كما لو تعهد بالمحافظة على كل من الأجهزة والبرامج وتحديثها. وإذا قام موظفو المؤجر بزيارة المستأجر للصيانة وتحديث البرمجيات فقد يتكمنون من الوصول إلى أيّ من البيانات وهذه القدرة تكون عرضية ولا تجعل المؤجر معالجاً؛ حتى عند رد الجهاز أو الأجهزة، قد يتمكن المؤجر من الوصول إلى بيانات غير مشفرة ولكنه ليس بمعالج.

كذلك، لنفترض أن الجهاز موجود في مباني مالكه ولكنه يسمح للغير بالحضور واستخدامه لمعالجة بياناته الخاصة في أي وقت يرغب به. وإذا كان للمستخدمين متطلبات محددة، يتحقق من الجهاز الذي يناسب احتياجاتهم ويوجههم إليه. يستطيع العملاء تثبيت أي نظام تشغيل وبرنامج يرغبون به، ويدفعون بحسب قوة الجهاز وسرعته ومدّة استخدامه.

كذلك، عندما يقوم بحفظ وتخزين أجهزة لأشخاص ثالثين لديه، ويمكنهم استخدامها في أي وقت يرغبون ويقوم هو بالصّيانة والمحافظة على الأجهزة وتحديث أنظمة التشغيل وضمان برامج الأمان.

كما، إذا كان لديه الكثير من المباني مع آلات مجهزة مسبقاً، يمكن عند الضرورة للعميل إحضار جهازه واستخدامه على طاولة احتياطية، أو قد يحضر USB تحمل البيانات واستخدام الموارد الموجودة.

لأسباب تتعلق بالمساحة والتكلفة، قد يشترك العديد من العملاء في جدول واحد مع وجود لوحات عامودية بينهم.

كذلك، قد يستخدم برنامج "Load Balancer" للتحليل أوتوماتيكياً وتحديد أي مبنى يحتوي على طاولات احتياطية. وأيٍّ منها لديها مساحة حرّة من أجل توجيه العملاء تلقائياً إلى الأماكن المناسبة. وهذا يسهل استخدام العملاء للموارد دون إضفاء صفة معالج على مقدم هذه الخدمة. كما وقد يوفر أجهزة تقدم نوعاً واحداً من برامج التطبيقات مثلاً البريد الإلكتروني، وإدارة علاقات العملاء... للعملاء الذين يرغبون فقط في تلك التطبيقات، وقد يسمح لموظفيهم وعملائهم بالفعل بزيارة المبنى حيث يحتفظ بالأجهزة لاستخدام الموارد المخصصة لذلك العميل. وقد يسمح للعملاء بتأجير البنية التحتية الخاصة به للآخرين أو مساعدتهم على استخدام الموارد.

وبشكل أساسي، تشبه هذه الحالات نماذج خدمة السّحابة. إن توفير أجهزة كمبيوتر مزودة بتطبيقات محددة مثبت مسبقاً مثل SaaS. إن توفير أجهزة الكمبيوتر حيث يمكن للعملاء تثبيت أنظمة التشغيل والتطبيقات التي يختارونها، والتي قد يأذنون لبعض موظفيهم أو عملائهم باستخدامها، يشبه IaaS. وأخيراً، إن توفير أجهزة الكمبيوتر التي يمكن للعملاء استخدامها لتطوير برامج التطبيقات الخاصة بهم، ونشر مثل هذه البرامج للاستخدام من قبل موظفيهم أو عملائهم هو مثل PaaS. إلّا أن السّحابة تتم باستخدام تكنولوجيا الـ Virtualization.[70]

النبذة الثانية: أنواع الخدمة المتوافرة

يمكن تعريف أنواع النشر على أنها طرق مختلفة يمكن من خلالها نشر البيانات. هذه الأنواع تتمحور حول المستخدم بشكل كامل، أي أنها تعتمد على متطلبات المستخدمين وراحتهم. في الأساس، هناك أربعة أنواع:

Private Cloud، Public Cloud، Community Cloud و Hybrid Cloud، ولكننا سنقوم بدمج Community Cloud و Private Cloud. يعتمد تصنيف هذه الأنواع على عدة عوامل مثل حجم السّحابة ونوع مقدم الخدمة والموقع ونوع المستخدمين والأمان وقضايا أخرى.

البند الأول: السّحابة الخاصة Private Cloud

بالنسبة لـ NIST السّحابة الخاصة أو Private Cloud يمكن تعريفها بأنها:

---

[70] Christopher Millard: "**Cloud Computing Law**", Oxford University Press, The Several Contributors, 2013, page 875-923 (Kindle Version).

“The cloud infrastructure that is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on off premises.”[71]

أي إنّ البنية التحتية الأساسية التي تستخدم حصراً من قبل شركة واحدة تضم العديد من المستهلكين وقد تكون مملوكة ومدارة من قبل الشّركة نفسها أو من قبل طرف ثالث أو مزيج من الإثنين وقد تكون موجودة داخل أو خارج مقر الشّركة.

يكون عادةً حجم هذه السّحابة أصغر من السّحب الأخرى وخاصةً عندما تكون مملوكة ومدارة من الشّركة عينها، عندها تكون هذه السّحابة آمنة جداً وللشركة كامل السّيطرة عليها أي أن الشّركة لا تعاني من المشاكل التي يمكن أن تواجهها في أنواع السّحب الأخرى، لكن مسألة إدارة وصيانة السّحابة داخل الشّركة مكلفة جداً وتفرض أعباء وخاصةً على الشّركات الصّغيرة أو الجديدة النشأة.

لكن عندما تكون السّحابة الخاصة موجودة لدى طرف ثالث تزداد المشاكل التي قد تواجهها الشّركة، فالسّحابة الآن هي أقل أماناً من وجودها في الشّركة فالطرف الثالث له السّيطرة على السّحابة. كذلك عند إخراج البيانات من الشّركة لدى شخص ثالث قد يكون خارج نطاق البلد وبالتالي تطرح مسألة النقل كما ومسألة القوانين المطبقة.[72]

ويمكن أن تكون السّحابة الخاصة مشتركة بين أكثر من شركة أو مستخدم يمكنهم لأسباب معينة المشاركة في هذه السّحابة، وتسمى عندها بالـ community cloud التي يكون نطاقها أكبر من نطاق السّحابة الخاصة. وهذه السّحابة هي مهمة للشركات التي لا يمكنها توفير تكاليف السّحابة ولا تثق في الوقت عينه بالسّحابة العامة.[73]

---

[71] Peter Mell, Timothy Grance, the NIST Definition of Cloud Computing (Recommendations of the National Institute of Standards and Technology), Special Publication 800-145, September 2011. (https://nvlpubs.nist.gov/nistpubs/legacy/SP/nistspecialpublication800-145.pdf)

[72] K. CHANDRASEKARAN: "**Essentials of Cloud Computing**", CRC Press, US, 2015, p. 51-52.

[73] **K. CHANDRASEKARAN**, opcit, p. 56.

البند الثاني: السّحابة العامة Public Cloud

عرّفتها NIST أنّها:

"The cloud infrastructure that is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic or government organization, or some combination of them. It exists on the premises of the cloud provider."[74]

أي أنها البنية التحتية السّحابية المعدة للاستخدام العام من قبل العامة. قد تكون مملوكة ومدارة من قبل شركة أو مؤسسة أكاديمية أو مؤسسة حكومية أو مزيج منها. وهي تكون موجودة في مقرّ مزوّد الخدمة.

تتكوّن السّحابة العامة من مستخدمين من جميع أنحاء العالم. يمكن للمستخدم ببساطة شراء الموارد والعمل بها متى أراد. ليس هناك حاجة إلى أي بنية تحتية مسبقة الإعداد لاستخدام السّحابة العامة. هذه الموارد متوفرة في مقر مزوّد الخدمة. عادةً يقبل مزوّدو الخدمة جميع الطلبات المرسلة.

بالرغم من أن لهذه السّحابة فوائد كثيرة، فإنها متوفرة للجميع وفي متناول يد العامة بسبب إمكانية دفع تكاليفها التي تعتمد على طريقة pay-as-you-go billing، ولها قواعد خدمة صارمة (SLA). لكن لها تحديات كثيرة، فهي تعتمد على الشّبكة أي أنها لا تعمل بدون الإتصال بشبكة الانترنت وأي خلل في الشّبكة لا يتحمله المزوّد ويتوجب على المستخدم الدفع حتى لو لم يحصل على الخدمة، كذلك مشكلة مكان تواجد البيانات والقوانين المطبقة لأنه عادةً تكون هذه السّحب موجودة خارج بلد الاستخدام خاصةً عند استخدامها من قبل من يتواجد في الدول النائية وغير المتقدمة.

أمّا التحدي الرئيسي لهذا النوع من السّحب هو الأمان وحماية البيانات، فهناك خشية اطلاع الغير على البيانات بالأخص عندما تكون تشريعات البلاد المتواجدة فيها البيانات تسمح بذلك.[75]

البند الثالث: سحابة مختلطة Hybrid Cloud

أتى تعريف NIST للسحابة وفق الآتي:

"The cloud infrastructure that is a composition of two or more distinct cloud infrastructure (private, community or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data

---

[74] Supra 71.

[75] **K. CHANDRASEKARAN**, opcit, p. 54-55.

and application portability (e.g., cloud bursting for load balancing between clouds)."[76]

بما معناه أنها البنية التحتية السّحابية التي هي تركيبة لبنيتين أو أكثر من البنى التحتية السّحابية (الخاصة أو العامة...) التي تبقى مكتسبة لصفة كيان مستقل، لكنها تكون مرتبطة ببعضها البعض وتمكّن من نقل البيانات والتطبيقات.

بما أن السّحابة المختلطة هي مزيج من السّحابة الخاصة والسّحابة العامة فهي بالتالي تدمج حسنات هاتين السّحابتين، كذلك سيئاتهما وتحدياتهما.

لتكوين هذه السّحابة، يكون هناك عادةً سحابة خاصة للمستخدم ويستعمل السّحابة العامة بسبب حاجته لموارد إضافية، يمكن اعتبارها إذاً سحابة خاصة ممتدة لسحابة عامة، ومثال على هذه السّحابة Eucalyptus التي هي أساساً سحابة خاصة ولكن اليوم هي سحابة مختلطة.[77]

الفقرة الثانية: الإستخدامات للحوسبة السّحابية

إن الحوسبة السّحابية هي جزء من العالم الإلكتروني وهو يسهلّ عمل كل الجهات المستخدمة لهذه التقنيات الحديثة، وتفتح مجالات عدّة للاستعمالات، فهي تكون أساساً لعديد من الإستخدامات الشّخصية والحكومية والمهنية، إن باستعمال التطبيقات التي تستند عليها كتقنية أو باستخدام فكرة السّحابة بحد ذاتها للتخزين. وهذا ما سوف نناقشه في هذه الفقرة الإستخدامات الثلاثة التي سبق ذكرها.

النبذة الأولى: الإستخدامات الشخصية

عند التكلم عن الحوسبة السّحابية على مستوى الفرد أي على مستوى الإستخدام الشخصي، نكون أمام فئتين من الاستخدامات: التخزين عبر الانترنت online storage والتطبيقات عبر الإنترنت online application.

1. التخزين عبر الانترنت

اليوم، استخدام الحوسبة السّحابية في تخزين البيانات خاصةً الشّخصية منها أكثر قوة من السّابق. فمن السّهل إنشاء البيانات والمعلومات وتحريرها: يتم حفظ البيانات تلقائياً وتكون سهلة الاسترداد، ويمكن الوصول اليها في أي وقت وفي أي مكان في العالم. يستطيع إذاً الفرد الوصول الى المعلومات والبيانات الموجودة على حاسوبه من أي جهاز استعمله، أينما استعمله ومتى استعمله. يقوم الفرد بحفظ معلوماته

---

[76] Supra 71.

[77] **K. CHANDRASEKARAN**, opcit, p. 61-62-63.

احتياطياً على السّحابة backing up data on cloud سواء على هاتفه، على حاسوبه، أو على أي جهاز يتصل بشبكة الانترنت، ويمكن لهذه البيانات أن تكون صوراً، فيديوهات أو معلومات مكتوبة.
و من أمثلة سحابة النسخ الاحتياطي cloud backup : Icloud, AmazonS3, Google Drive, dropbox.[78]

2. التطبيقات عبر الانترنت

تستخدم معظم التطبيقات والمواقع الإلكترونية التي يستخدمها الفرد على الهاتف وأجهزة الكمبيوتر تقنيات الحوسبة السّحابية المستضافة. فمثلاً عند مشاهدة فيلم على الانترنت بجودة عالية وبث مباشر فذلك بفضل كون الموارد مستضافة على سحابة ولهذا السّبب الكثير من مواقع بث الفيديوهات يوفر خيار تشغيل نفس الفيلم على أكثر من خادم. كذلك عند استخدام التطبيقات المتعلقة بالتواصل الاجتماعي تحفظ المحادثات والمعلومات المدخلة على سحابة مزود الخدمة وليس على جهاز الفرد الشّخصي. يمكن تقييم استخدام التطبيقات كالآتي:

أ. تشات بوت Chatbots[79]

Siri, Alexa, Google Assistant برامج chatbots الذكية تستند الى لغة طبيعية. تستفيد هذه الـchatbox من إمكانية السّحابة من توفير خبرات شخصية ذات صلة بالموضوع. فكل مرّة نقول فيها "hey Siri!" يجب أن نكون على علم أنها قائمة على حل AI[80] مبني على السّحابة.

ب. التواصل

السّحابة تسمح للمستخدمين بالوصول إلى أدوات اتصال على الشبكة كرسائل البريد الإلكتروني والتقاويم. تعتمد معظم تطبيقات المراسلة مثل skype وwhatsapp أيضاً على البنية الأساسية السّحابية. ومن خلال حفظ المعلومات والرسائل على أجهزة مزود الخدمة تتاح للشخص إمكانية الوصول إليها من أي مكان عبر الانترنت.

---

[78] Vijay Kumar: "**Powerful Uses Of Cloud Computing**", February 24, 2018, published on klientsolutech.com.
(Available at: http://www.klientsolutech.com/powerful-uses-of-cloud-computing/)
(Accessed on 4 September 2018, at 08:14 AM).

[79] برامج الكترونية مصنوعة لإجراء محادثات مع أشخاص طبيعيين وخاصةً عبر الانترنت

[80] AI: Intelligence artificielle

ج. شبكات التواصل الإجتماعي

تطبيقات التواصل الإجتماعي هي الأكثر شعبية وعادةً مايتم تجاهلها من الحوسبة السّحابية. فالعديد من التطبيقات كـ Facebook; Twitter; LinkedIn و MySpace تستخدم الحوسبة السّحابية. تم تصميم مواقع التواصل الإجتماعي للعثور على الأشخاص اللّذي يعرفهم الفرد أو يريد التعرف إليهم والتواصل معهم ومشاركتهم الصّور وغيرها، وأثناء البحث ينتهي الافراد الى مشاركة الكثير من المعلومات الشّخصية. فلا يشارك الشّخص المعلومات فقط مع الذي يتواصل معه ولكن مع صانعي النظام الأساسي (platform maker) أي على السّحابة التي يكون مشتركاً بها في جهاز مزوّد سحابي. بمعنى آخر المعلومات تكون بحوزة المؤسس الأساسي للتطبيق وبحوزة مزود خدمة السّحابة المشترك بها المؤسس إلا إذا كان لهذا الأخير سحابة خاصة به أو datacenter خاص وغير مشترك بخدمة السّحابة. وهذا يطرح الكثير من الإشكاليات التي ستطرح وستعالج لاحقاً في الدراسة.

النبذة الثانية: الإستخدامات الحكومية

لكي تتمكن الحكومة من إستخدام السّحابة يجب أن تكون حكومة إلكترونية في الأساس أو لن تكون بحاجة لمثل هذه التقنية فتشكّل أعباء إضافية دون الإستفادة من هدف هذه الخدمة. ولكن ماهي الحكومة الإلكترونية؟ وما هو الواقع اللّبناني في ما خصّ الحكومة الإلكترونية؟ وما هو موقع لبنان بين الدول الأخرى في هذا الإطار؟

البند الأول: الحكومة الإلكترونية

لتتمكن الحكومة أو الدولة من الاستفادة من خدمة السّحابة يجب أن تكون أولاً حكومة إلكترونية، فماهي الحكومة الإلكترونية أو الـ E-Government؟ وكيف يمكن للحكومة الإستفادة من السّحابة؟

يشير حرف "e" في كلمة e-government إلى النظام الأساسي والبنية التحتية الإلكترونية التي تمكن من إنشاء الشّبكة الإلكترونية ونشرها وتشغيلها.

تعرّف منظمة الأمم المتحدة ONU الحكومة الإلكترونية على أنها استخدام تكنولوجيا المعلومات والاتصالات (TIC) لتحسين أنشطة منظمات القطاع العام وعملائها. ويمكن توجيه هذه الجهود نحو توفير الخدمات للمواطنين أو تحديث ممارسات العمل وتحقيق وتحسين كفاءة العمّال[81].

[81] Driss Kettani and Bernard Moulin: **E-Government for Good Governance in Developing Countries**, New York and UK, Anthem Press, 2014. (Available at: https://www.idrc.ca/sites/default/files/openebooks/561-8/index.html#ch01lev01) (Accessed on 26 August at 21:45 PM).

كما وعرّفت الـ OECD الحكومة الإلكترونية بأنّها "استخدام تكنولوجيا المعلومات والاتصالات وخاصةً الإنترنت من أجل تحقيق حكومة أفضل". هذا التعريف يركز على سبب قيام البلدان بتنفيذ الحكومة الالكترونية بدلاً من أدوات تكنولوجيا المعلومات والاتصالات نفسها. في مواجهة الضغط الناجم عن زيادة أداء الحكومة مع الاستجابة لاحتياجات المواطن، أدركت دول منظمة التعاون الاقتصادي والتنمية (OECD) أن الحكومة الالكترونية تتجاوز مجرد وضع المعلومات والخدمات عبر الانترنت، ويمكن استخدامها كأداة لتحويل الهياكل وجعلها أكثر كفاءة وموجهة للمستخدم وشفافة[82].

الأهداف الرئيسية من استراتيجية الحكومة الإلكترونية هي: الوصول إلى الخدمات والاختيار، مشاركة المواطنين والخصوصية ووضع استراتيجية شاملة:

1. الوصول إلى الخدمات: يجب على الحكومات اتباع سياسات لتحسين الوصول إلى الخدمات عبر الإنترنت. في الواقع، إن معظم المواطنين يريدون ببساطة الوصول بشكل أفضل إلى الخدمات العامة، بأسرع وسيلة وبكفاءة عالية.
2. الاختيار: يجب أن يكون لدى العملاء حرية اختيار طريقة التفاعل مع الحكومة. يجب ألّا يقلل اعتماد الخدمات عبر الانترنت من هذا الخيار. فالمواطن الذي يريد ويفضل التعامل التقليدي الورقي يجب ألّا يحرم من هذا الخيار.
3. إشراك المواطنين: تحتاج خدمات معلومات الحكومة الإلكترونية إلى إشراك المواطنين في عملية حوسبة الإدارة. ستساعد آليات المراقبة في تحسين استخدام المعلومات وتعزيز مشاركة المواطنين.
4. الخصوصية: يجب ألّا يتم تسليم الحكومة الإلكترونية على حساب الخصوصية ويجب الإنتباه إلى حماية خصوصية المستخدم/المواطن وسياسته ومساءلته[83].

---

[82] OECD, **Background paper: Implementation E-government in OECD countries: experiences and challenges** (Available on: www.oecd.org/mena/governance/36853121.pdf) (Accessed on August 26, 2018 at 22:10 PM).

[83] Georges Labaki: "**Le gouvernement electronique: visions et strategies pour le cas libanais**", 2011, publié sur lebarmy.gov.lb. (Available at: https://www.lebarmy.gov.lb/fr/content/le-gouvernement-electronique-visions-et-strategies-pour-le-cas-libanais) (Accessed on 28 August, 2018 at 15:32 PM).

البند الثاني: الواقع في لبنان وبعض الدول

في الواقع، منذ إنشاء وحدة التعاون الفني في مكتب وزير الدولة لشؤون التنمية الإدارية (OMSAR) [84] في عام 1994، كان تطوير "الحكومة الإلكترونية" هو الهدف الإستراتيجي للدولة اللّبنانية.

عند النظر إلى الوضع الإلكتروني للوزارات في لبنان، نرى أنه على 30 وزير، 7 من أصلهم ليس لديهم مواقع على الإنترنت "gov.lb." وهم:

-نائب رئيس المجلس

-وزراء الدولة السّتة (بواقع أنهم بدون حقيبة، يمكن فهم أن اتصالاتهم ليست بحاجة إلى موقع).

كذلك هناك العديد من المواقع الإلكترونية المتعلقة بمؤسسات حكومية أو تابعة للدولة اللّبنانية التي تنتهي بـ"gov.lb." أو غيرها كـ "org.lb."، وكل ذلك لتطوير الخدمة العامة وتسهيلها على المواطن. وبهذا السّياق يمكننا ذكر موقع dawlati.gov.lb التي أصبح البوابة الحكومية للدولة، أطلقه وزير الدولة لشؤون التنمية الإدارية، هذا الموقع يتضمن: معلومات حول المعاملات الإدارية وموضوعها والمستندات المرفقة بها وآلية سير العمل ومدّة إنجازها والرسوم المتوجبة كما ويتضمن استمارات إلكترونية للتحميل وللطباعة ومنها للتعبئة والطباعة[85].

إلّا أننا نرى أنه ليس هناك من بنية موحدة لجميع المواقع، فمنها ما يظهر logo العلم اللّبناني ومنها ما يظهر الأرزة اللّبنانية، كذلك منها ما يقدم المعلومات باللّغتين العربية والفرنسية، ومنها باللّغتين العربية والإنكليزية ومنها باللّغات الثلاث المذكورة. يجب توحيد هذه المواقع إذ إنها تتعلق بحكومة واحدة وبدولة واحدة، وليست لوزارة واحدة.

كذلك هذه المواقع لا تعطي المواطن الحق بتعبئة وتقديم معاملاته بطريقة إلكترونية موفرة عليه الوقت والمسافة معتمدة على اللّامركزية بالمعاملات الإدارية بشكل خجول. إلّا أن وزارة الصّحة اللّبنانية أطلقت مؤخراً في عام 2018 بالاشتراك مع جمعية "لبنانيون" اللّبنانية والسّفارة الأميركية في لبنان، الخدمات الرقمية للوزارة أي إمكانية تعبئة وتقديم وإتمام 70% من المعاملات المتعلقة بهذه الوزارة إلكترونياً[86]. كذلك وزارة المالية تعطي المواطنين إمكانية تقديم التصاريح المتعلقة بشركاتهم ومؤسساتهم الدورية والسّنوية عبر الموقع المحدد لوزارة المالية، وإمكانية تسديد الضرائب بواسطة الدفع الالكتروني عبر بطاقات الائتمان والتحويل المصرفي منذ عام 2013.[87]

---

[84] OMSAR: Office of Minister of State for Administrative Reform.

[85] مكتب وزير الدولة لشؤون التنمية الإدارية، **سياسات وبرامج وإجراءات لخدمة عامة متميزة**، التقرير السّنوي لعام 2014-2015، ص. 48-49.

[86] https://www.moph.gov.lb/ (Accessed on August 16, 2018 at 09:30 AM).

[87] http://www.dawlati.gov.lb/news-detail/-/asset_publisher/TnfLM2HDHkp4/content/launching-of-taxes-e-payment-service. (Accessed on August 16, 2018 at 10:05 AM).

بحسب تصنيف الـ UN لسنة 2018 للدول المعتمدة الحكومة الإلكترونية، أتى لبنان في الموقع التاسع على 19 بلد في منطقة الـ MENA [88] وموقع الـ 99 على 193 بلد على الصّعيد العالمي[89] بعد أن كان في المركز 73 عام 2016[90]، وبذلك نرى أن على الدولة اللّبنانية والحكومة العمل لتحسين الحكومة الإلكترونية إذ إن لبنان قد تراجع 26 موقع خلال سنتين.

فيجب العمل على تكوين بنية تحتية كما وتطوير إمكانية إتمام المعاملات الرسمية إلكترونياً وليس فقط الحصول على الوثائق، كذلك تطوير التشريعات المتعلقة بالموضوع. أمّا بالنسبة للبنية التحتية، يمكن للدولة إنشاء داتا الحكومة الضخمة Big Data Government بدلاً من الـ Datacenter أو الـ servers لكل وزارة على حدة. أو يمكنها الإنتقال تدريجياً إلى السّحابة الإلكترونية من أجل تأمين القدرة الحاسوبية ومراكز البيانات حسب الطلب لمختلف الأجهزة الحكومية والوزارات[91].

فالكثير من الدول وضعت استراتيجيات وانتقلت إلى السّحابة:

1. حكومة المملكة المتحدة UK Government

في عام 2010، نفذت المملكة المتحدة استراتيجية G-Cloud لتحقيق الكفاءة الإقتصادية والإستدامة لعمليات تكنولوجيا المعلومات والإتصالات الحكومية. تم اتخاذ المبادرة من خلال اعتماد الحوسبة السّحابية وتوفير موارد الحوسبة. وقد أشير على وجه التحديد إلى أن المبادرة ستحدث تغييرات أساسية في القطاع العام. توضح هذه الإستراتيجية بالتفصيل كيف ستحقق الحكومة هذا على النحو التالي:

أ. تقديم أنظمة ICT تتسم بالمرونة والاستجابة للطلب من أجل دعم السّياسات والاستراتيجيات الحكومية.

ب. الإستفادة من التكنولوجيا الجديدة لتقديم خدمة أسرع وتخفيض التكاليف.

ت. تلبية الأهداف والاستدامة البيئية.

ث. السّماح للحكومة بالحصول على طريقة تشجع سوق الموردين وتدعم الموردين الناشئين.[92]

2. حكومة الإمارات العربية U.A.E

---

[88] MENA: Middle East and North Africa

[89] https://publicadministration.un.org/egovkb/en-us/Data/Country-Information/id/94/Lebanon/dataYear/2018. (Accessed on August 16, 2018 at 10:30 AM).

[90] https://publicadministration.un.org/egovkb/en-us/Data/Country-Information/id/94-Lebanon/dataYear/2016. (Accessed on August 16, 2018 at 11:22 AM).

[91] عباس بدران، **عصر الفرص الجديدة: الحكومة الذكية**، الدار العربية للعلوم ناشرون، 2014.

[92] Sean Rhody and Dan Dunn: "Government Cloud", published in **Encyclopedia of Cloud Computing**, John Wiley & Sons Ltd., United Kingdom, 2016, p. 59-60.

لقد اعتنقت هذه الحكومة السّحابة في سنوات 2013-2014 وذلك بعد إطلاق استراتيجية 2012-2014. وهذه الحكومة هي الرائدة في الشّرق الأوسط في استعمال تقنيات الـ ICT ولكن اعتناق السّحابة يعود إلى أربع أو خمس سنوات فقط.

وبما أنها من الدول الرائدة، أعلنت AWS من Amazon أنها ستفتتح أول Datacenter لها في الشّرق الأوسط في Dubai سنة 2019.[93]

وعودةً للوضع الراهن في لبنان، على الحكومة اللّبنانية وضع استراتيجية واضحة تتعلق بهذا الشّأن كون الحياة الالكترونية هي الرائدة اليوم وغداً. ويجب دراسة ماهية المعلومات التي لا تتسم بالسّرية والتي يمكن أن تكون على سحابة عامة وبالتالي توفر الحكومة من النفقات أكثر، فمثلاً يمكن وضع نتائج الامتحانات الرسمية على السّحابة العامة، إذ إنها لا تنشر سوى مرّة في السّنة فتسمح للطلاب الدخول الى الموقع ومعرفة نتائجهم دون أية صعوبة، ففي الحالة الحالية عند وجود ضغط على الـ servers في وزارة التربية لا يستطيع الجميع الوصول الى نتائجهم بسبب نسبة استيعاب الـ servers للضغط، كما وأنها لا تتسم بالسّرية. ولكن هناك معلومات وبيانات لا يجوز إلّا أن تكون في سحابة خاصة داخل الدولة أكانت سحابة حكومية أو خدمة مقدمة من مزوِّد وذلك لكي لا يكون هناك لدولة أخرى سلطة عليها، كالمعلومات الشّخصية للأشخاص.

كذلك إن إنشاء الدولة لسحابة حكومية وفتح السّحابة للعامة سيؤدي إلى دخول مردود كبير على الدولة فيمكن استغلالها كقطاع الكهرباء وغيره. ولكن لإنشاء قطاع كهذا يجب دراسته معمقاً وتأليف وزارة مختصة به يمكن تسميتها وزارة لشؤون الحكومة الإلكترونية والتطور. بالإضافة إلى الفوائد الأخرى المتعلقة بالخدمة العامة واستفادة المواطنين منها بأسهل وأسرع الوسائل.

ولكن إذا انتقلت الدولة إلى سحابة مقدمة من شركة خاصة، يجب وضع الكثير من الإشكاليات قيد الدرس، كالسّرية، الأمان، مكان تواجد الـ servers، النفقات... إذ عليها للتوفير الإستفادة من الخدمات وإعادة استعمالها أكثر من مرّة. وسنتكلم عن هذه النقاط لاحقاً، فهي نقاط موحدّة ما بين جميع الاستخدامات.

---

[93] Debbie Garside: **Moving the Middle East to the Cloud: why it is time to seize the opportunity**, 21 November 2017, published on: cloudcomputing-news.net. (https://www.cloudcomputing-news.net/news/2017/nov/21/moving-middle-east-cloud-why-it-time-seize-opportunity/) (Accessed on 28 August 2018 at 18:14 PM).

النبذة الثالثة: الإستخدامات المهنية

مع دخول الحوسبة السّحابية الواقع الحالي، دخلت الحياة المهنية أيضاً وأصبحت ضرورة للشركات. فلن نقوم بذكر الكثير من المهن، سيقتصر الحديث عن المصارف وعن مهنة المحاماة والبيانات في الشّركات التي توضع على السّحابة، إذ إن جميع المهن والشّركات تتشابه في أسباب إنتقالها للسحابة والمخاوف والوقاية التي يجب أن تأخذها قبل الانتقال. ولكن بما أن للمصارف في لبنان خصوصية وهو القطاع الأكثر تأثيراً على الوضع في لبنان، وبما أننا بصدد دراسة قانونية يجب التحدث عن أهمية هذه الخدمة في حياة القانونيين المحامين.

1. مهنة المحاماة

بدأت مكاتب المحاماة، بشكل متزايد، في اوروبا وفي اميركا وغيرها من الدول، بالانتقال الى السّحابة. يعكس هذا الحاجة للسوق لمرونة تكنولوجيا المعلومات التي تتسم بالموثوقية والأمان والفعالية من حيث التكلفة. فهذا الانتقال يوفر خدمات النسخ الاحتياطي واستعادة البيانات في حالات الكوارث. بالرغم من الفوائد العديدة، إنّ هناك معتقداً يصنفه البعض بالخاطئ وهو أن السّحابة تمثّل خطراً على مكاتب المحاماة إذ إن تخزين البيانات السّرية ومعلومات العميل في السّحابة هو في الواقع إجراء أمني قابل للحماية من كل الكوارث البشرية والطبيعية.

إن السّحابة تقدم لمكاتب المحاماة وسيلة فعّالة لتخزين كميات كبيرة من البيانات بطريقة سهلة وفعّالة. عند التنفيذ السّليم، تمكن السّحابة المحامين من العمل من أي مكان، مما يؤدي إلى زيادة الإنتاجية وتعزيز التوازن بين العمل والحياة. خاصةً مع التطبيقات التي تقدمها شركات السّحابة فتسهل ولوج المحامي إلى بياناته وبيانات أخرى يريدها، بالأخص أن المحامي بحركة دائمة، فهو مثلاً في لبنان ينتقل من دائرة إلى أخرى، من قصر عدلٍ إلى آخر، فيمكنه الإستفادة من وقته في الدوائر أو وقته المتفرغ، كذلك المحامي غير القادر على القدوم إلى المكتب وخاصةً المتدرج يمكنه العمل من منزله وإبقاء المحامي على اطلاع باللّوائح عند استخدام تطبيق Microsoft Office.

بالإضافة إلى تقليل مصاريف المكتب وذلك مع تقليل الخوادم في المكتب وتقليل تكاليف الصّيانة. ولكن الإنتقال إلى السّحابة يجب أن يتم بعناية وأن يعرف المحامي الخيارات المتاحة له لضمان أن يكون إنتقاله إلى السّحابة أكثر أماناً وامتثالاً.[94]

---

[94] Monica Brink: **The Ruling On Cloud Computing: Analysing the Legal Perspective**, 17 February 2017, published on cloudcomputing-news.net.
(Available at: https://www.cloudcomputing-news.net/news/2017/feb/17/ruling-cloud-computing-analysing-legal-perspective/) (Accessed on 24 August 2018 at 19:21 PM).

2. المصارف

عادةً تحب المصارف الإحتفاظ بتقنية المعلومات الخاصة بها في قبوتها، ولذلك غالباً ما تكون حذرة من استخدام السّحب العامة والمختلطة. ولكن لاحقاً مع تطور الحوسبة السّحابية وزيادة نسبة الأمان فيها، انتقلت البنوك إليها، كما وعليها موجب تلبية رغبة العملاء بالحصول على الخدمات من منازلهم وإتمام معاملاتهم دون الحاجة للذهاب إلى مركز المصرف الرئيسي أو الفرع. [95]

لكي يتمكن المصرف من تقديم خدمة مناسبة يجب توفير بنية تحتية لتكنولوجيا المعلومات، فالكثير منهم كبنك عودة يقوم بإنشاء سحابته الخاصة التي قد تقدم خدمتها للعامة. كذلك الكثير من المصارف التي لا تستطيع بناء سحابتها الخاصة قد تلجأ إلى الشّركات التي تقدم خدمة السّحابة ولكن هناك شروط مفروضة من مصرف لبنان أهمها السّرية المصرفية، فلا يجب أن تخرج البيانات إلى خارج النطاق اللّبناني لكي لا تكون تحت سلطة قانون دولة أخرى، فجاءت شركة Cirrus اللّبنانية بالحل المناسب للمصارف، فـ servers هذه الشّركة موجودة في لبنان وبالتالي البيانات والمعلومات الموجودة عليها موجودة في لبنان، كما أن موظفي هذه الشّركة يخضعون لشروط السّرية المصرفية كموظفي المصارف، وقد سبق لها أن تعاملت مع مصرف لبناني، فهي تؤمن خدمة السّحابة لمصرف Saradar Bank.[96]

المبحث الثاني: إبرام العقد وحماية المتعاقد الضعيف

بعد أن قام المستخدم بإختيار نوع الخدمة التي تناسبه والشّركة التي يريد التعامل معها وبإيلائها ثقته في البيانات التي تتعلق به أو بعمله، سيقوم هذا الشّخص مهما كانت صفته بإبرام عقد مع الشّركة المختارة. فتختلف طريقة إبرام العقد بين مستخدمٍ وآخر بحسب ما سنرى في هذا المبحث؛ كما وأن هذا الإختلاف، يؤدي إلى وجود مجموعة من المستخدمين التي يمكن أن نصفها بضعيفة والتي تتطلب حمايةً وإهتماماً من قبل المشرّع.

[95] Nick Ismail: **Why do Banking institutions no longer fear the cloud?**, 22 May 2018, published on: information-age.com. (Available at: https://www.information-age.com/banks-cloud-123472507/) (Accessed on 25 August 2018 at 8:12 AM).

[96] ITG: **First Ever on a National Private Cloud! Our Affiliates Cirrus and IMS Provided Saradar Bank with a Cloud Managed Platform to Run the Bank's Core Services**, Beirut, December 4, 2017, Published on: itgholding.com.
(Available on: http://www.itgholding.com/news/403/first-ever-on-a-national-private-cloud-our-affiliates-cirrus-and-ims-provided-saradar-with-a-cloud-managed-platform-to-run-the-banks-core-services/) (Accessed on September 13, 2018 at 14:22 PM).

الفقرة الأولى: إبرام العقد

كما سبق وذكرنا في الفقرات السّابقة، يتم تنظيم تقديم خدمات الحوسبة السّحابية بعقد أو مجموعة عقود تحكم العلاقة التي سترتبط كلّاً من الطرفين ويمكن أن تكون عقوداً نموذجية أو عقوداً يمكن التفاوض على بنودها، إلّا أن هذين النوعين من العقود قد يحتويان على نفس البنود مع شروط مختلفة، فسوف نتكلم عن العقود النموذجية والبنود التي ترد بها ومن ثم عن العقود المفاوض عليها والبنود التي غالباً ما يفاوض عليها.

النبذة الأولى: العقود النموذجية

تنقسم العلاقة بين مزود الخدمة والمستخدم إلى فئتين واضحتين، اعتماداً على ما إذا كانت الخدمة المقدمة مدفوعة أو مجانية. ومع ذلك، هذا التمييز غير واضح. على سبيل المثال، قد تفرض بعض الخدمات "المجانية" تكاليف غير مالية على العميل كالإعلان السّياقي أو فرض شروط الترخيص التي تسمح للمزوِّد بإعادة استخدام بيانات العميل لأغراضه الخاصة. كذلك الخدمات المدفوعة تتدرج بين تلك التي يتم الدخول إليها على أساس عقد النموذج الموحد للمزوّد وتلك التي يتم فيها التفاوض على شروط العقد بشكل كامل اعتماداً على قوة المساومة للمزوّد والعميل.[97]

كذلك الحوسبة السّحابية تشكل عادةً تعاقداً إلكترونياً وكون التعاقد الإلكتروني يستخدم عقوداً نموذجية في أغلب الأحيان فيفرض النموذج على أساس الموافقة أو الترك Take-it-or-leave-it basis. لذلك، تصبح "عدم قابلية التفاوض" الميزة الأكثر أهمية ولا تترك مجالاً أمام المستهلك للمراجعة أو التفاوض على هذا العقد. فالعملاء الذين يحاولون قراءة بنود العقود الإلكترونية تعتريهم صعوبة في فهم الصّفحات المليئة بالمصطلحات القانونية التي يصعب على محامٍ خبير حلّها وفهمها.[98]

علاوة على ذلك، تكون هذه العقود مصاغة بطريقة لحل جميع المشاكل التي يمكن أن يواجهها المزوّد. الطريقة الشّائعة للموافقة على عقد السّحابة هي التعاقد بالنقر. المقصود هو تعبير المستخدمين عن موافقتهم على الشّروط التي تقدمها عن طريق النقر على زر "أوافق" "I accept"، "نعم" "Yes" أو "أنا موافق" "I agree".[99] فهذه الطريقة في الاتفاق هي الحل لمتطلبات مقاربة العقد وأيضاً تمكين الشّركات

---

[97] Simon Bradshaw, Christopher Millard and Ian Walden: **"The terms they are A-changin'… watching cloud contracts take shape, the center for technology innovation"**, issue in technology innovation, 2011, page 15.

[98] Robert Hillman: **"Standard-form contracting in the Electronic Age"**, N.Y.U.L.Rev.429.2002, page 479.

[99] Maryke Silalah Nuth, **"E-commerce Contracting: the effective formation of online contracts"**, university of Oslo, 2011, page 118.

من إبرام العقد على الفور. وهنا يطرح التساؤل هل تتوفر في مثل هذه الحالات إرادة التعاقد؟ فكما سبق ورأينا أن هذا عقد إذعان، وللمستخدم العديد من الإحتمالات فإذا إرتأى أن هذه الشّروط لا تتناسب معه، يمكنه التعاقد مع شركة أخرى قد تقدم شروط أنسب، وبالتالي إرادة المتعاقد متوفرة إذ بالإضافة إلى كل ما أتينا على ذكره يمكنه الرفض وليس ملزماً بالموافقة.

العقود النموذجية غالباً ما تعرف بالـ Terms and Conditions (T&C) أي الأحكام والشّــروط، وهـذه الـ T&C تأتي بعدّة أشكال، أحياناً تكون بسيطة ومختزلة وأحياناً طويلة ومعقدة[100]. يقدم بعض مزوّدي الخدمات السّحابية مستنداتهم متكاملةً والبعض الآخر يقسّمها على عدّة وثائق، فهم يقدمون المستندات التالية:

- شروط الخدمة Terms of Service (ToS): عادةً ما تكون أهم مستند في العقود الإلكترونية وكذلك عقود الحوسبة السّحابية. تشرح الـ ToS أحكاماً مهمة مختلفة مثل نطاق الخدمة السّحابية والتزامات الموفر وحقوق الملكية الفكرية والبنود المتعلقة بالبيانات أو المحتوى في الخدمة السّحابية والقانون المطبق والصّلاحية القضائية وإنهاء العقد.
- اتفاق مستوى الخدمة Service Level Agreements (SLA): إنها تصف المستوى المحدد للخدمة، خيارات الدعم، المستوى المضمون لأداء النظام في ما يتعلق بوقت التوقف أو الجهوزية بالإضافة إلى الرسوم.
- سياسة الإستخدام المقبول Acceptable Use Policy (AUP) : يوضح هذا المستند الإستخدامات المسموح بها وكذلك الإستخدامات المحظورة للخدمة، وذلك وفق السّلوك الأخلاقي والسّلوك القانوني.
- سياسة الخصوصية Privacy Policy: هذا المستند يحكم عادةً التعامل مع المعلومات الشّخصية.[101]

على الرغم من أن بعض مزوّدي الخدمة يقدمون جميع هذه المستندات، من الشّائع جداً أن نرى AUP مطويّة في ToS، في حين أن العديد من الخدمات حتى تلك المدفوعة لا تقدم SLA.[102]

[100] Simon Bradshaw, Christopher Millard and Ian Walden: **“Contracts for clouds: comparison and analysis of the Terms and Conditions of Cloud Computing services”**, centre for commercial law studies, London, 2010. (Available at: https://ssrn.co/abstract=1662374) (Accessed on August 1, 2018 at 10:09 AM).

[101] Unknown (Candidate number: 8024): **Drafting a Cloud Computing Contract**, university of Oslo faculty of Law, 2011, page 14.

[102] Supra 97, page 14.

أمّا بالنسبة لتعديل هذه الشّروط، يزعم العديد من مقدمي الخدمة قدرتهم على تعديلها من جانب واحد ومن ثم نشر نسخة محدثة على مواقعهم، أو تقديم إشعارٍ مكتوبٍ عندما يكونون على وشك إجراء تعديل على البنود.[103] ولكن في بعض الأحيان أيضاً لا يعطى المستخدم علماً بتعديل البنود ولا يمكنه معرفة آخر تحديث إلّا من خلال مقارنة بنود الـ T&C في المستندين القديم والجديد كل فترة زمنية الأمر الذي لا يقوم به المستخدمون.

النبذة الثانية: العقود أو البنود المفاوض عليها

بالرغم من شيوع العقود النموذجية لإبرام عقد خدمة السّحابة، فإنّ بعض هذه العقود يتم التفاوض عليها بطريقة مماثلة لعقود التعهد التقليدية وذلك بسبب قيمتها أومخاطرها أو مظهرها العام على سبيل المثال لا الحصر.

كذلك مفاوضة العقود يكون حسب حجم الشّركة المزوّدة، فإذا كانت الشّركة كبيرة وكان العقد لا يتمتع بالصّفات المذكورة في المقطع السّابق فتفرض الشّركة شروطها ولا تقبل المفاوضة. أمّا عندما تكون الشّركة صغيرة أو جديدة النشأة، فقد تقبل بالمفاوضة على العقود وذلك لجذب عدد من المستخدمين.

أمّا من ناحية المستخدمين، سواء كانت شركة كبيرة أم صغيرة فيكون سبب طلبهم إمّا داخلياً أم خارجياً. فالأسباب الداخلية تشمل القضايا التجارية مثل مستويات الخدمة العالية المطلوبة للخدمات الحرجة، وتخصيص المخاطر بين المستخدم والمستفيد (وخاصةً مسؤولية المزوِّد). أمّا بالنسبة للأسباب الخارجية الرئيسية، كالإمتثال للقوانين والأنظمة بما في ذلك الإجراءات التنظيمية في البلد التي تكون موجودة ومسجلة فيه الشّركة، مثلاً إذا كان هناك مانع من التعامل مع إحدى البلاد يمكن أن تتضمن الشّروط إلغاء الخدمة إذا انتقلت ملكية الشّركة إلى شخص من جنسية هذا البلد، أو إذا دخل شريك فيها من هذه الجنسية وغيرها من الحالات التي قد تضع المستخدم في وضع حرج بالنسبة للإمتثال التنظيمي في بلاده. ومع ذلك، هناك عوامل خارجية أخرى مثل شركات التأمين التي قد يزداد دورها في تطور سوق السّحابة فقد تُصِرّ مثلاً على شهادات معينة قبل الموافقة على تأمين الخدمات.[104]

قد يقرر المستخدمون أنه بالنسبة للخطط التجريبية الأولية الصّغيرة أو اختبارات الإنتقال إلى السّحابة، فإنهم بغنى عن خسارة الوقت وتكاليف المفاوضة. على سبيل المثال كان برنامج alpha.gov.uk من أصل موقع واحد في المملكة المتحدة يعتمد على خدمة IaaS من Amazon على أساس العقد

---

103 Ibid page 2.

104 W. Kuan Hon, Christopher Millard & Ian Walden: "**Negotiating Cloud Contracts: Looking At Clouds From Both Sides Now**", Stanford Technology Law Review, Volume 16, Number 1, Fall 2012, Page 86.

النموذجي والموافقة عبر النقر. عند الرغبة في الانتقال الكامل للسحابة أو معالجة البيانات الخاصة الشّخصية، قد يقوم هؤلاء المستخدمون بالتدقيق بشروط العقد وبالمفاوضة عليها. قد يقومون بالمفاوضة على الشّروط دون الاستعانة بمحامٍ إلّا وقت الوصول إلى بنود قانونية وعندها يصعب على المحامي المفاوضة بعد الاتفاق بين المزوّد والمستخدم.

بالإضافة إلى أن الكثير من المستخدمين يفضلون الإشتراك بالخدمة عبر الوسيط إذ إن لديه القدرة على التفاوض مع مزوّد الخدمة بسبب نوع العلاقة الدائمة التي تربطه به. فالوسيط على علاقة بالطرفين كما سبق وذكرنا، فيمكنه شراء الخدمة وإعادة بيعها للمستخدمين وعلى هذا الأساس يمكنه تعديل بعض الشّروط وتحملها.

عادةً تكون البنود المفاوض عليها التالية:

1. مسؤولية المزوّد عن الاحتفاظ بالبيانات وإضاعتها أو تلفها.
2. المرونة والتوافر والأداء ومستويات الخدمة.
3. القضايا التنظيمية: تصدير البيانات وموقعها ومعالجتها.
4. السّرية والأمان.
5. إنهاء العقد.

وجميع هذه النقاط ستعالج لاحقاً في القسم الثاني، مبينين أسباب طلب التعديل والتفاوض.

الفقرة الثانية: حماية المستهلك

بادئ ذي بدء يجب تعريف المستهلك خاصةً في إطار الحوسبة السّحابية، هل هو نفس تعريف المستهلك في العقود التقليدية؟ أم أن هناك بعض الإختلافات؟ ولكن تعريف المستهلك ليس ما يهم، إنما الأهم هو معرفة الحماية الموجودة في القانون الوضعي في ما يخص إبرام هذا المستهلك لعقد السّحابة.

النبذة الأولى: مفهوم المستهلك في الحوسبة السّحابية

يعرّف المستهلك في اللّغة بأنه من استهلك المال أو الشّيء، أي من انفق المال أو الشّيء أو أنفذه.[105] أمّا قانوناً يقصد بالمستهلك وفقاً للمشرع اللّبناني "الشّخص الطبيعي أو المعنوي الذي يشتري خدمة أو سلعة أو يستأجرها وذلك لأغراض غير مرتبطة بنشاطه المهني."[106]

نلاحظ من هذا التعريف شموله للشخص الطبيعي والمعنوي كما فرضه شرطاً لاعتباره مستهلكاً وهو أن يكون الغرض من التعاقد الاستهلاك الشّخصي وليس المهني.

---

[105] المنجد في اللّغة والأعلام، دار المشرق للنشر، بيروت، 1986، ص. 871.

[106] نص المادة 2 من قانون حماية المستهلك اللّبناني (قانون رقم 659 تاريخ 4 شباط 2005).

كذلك التعريف الفقهي ذهب في البدء في تقسيمه إلى اتجاهين: اتجاه واسع وقصد به كل شخص يتعاقد بهدف الاستهلاك أي بهدف استعمال أو استخدام مال أو خدمة سواء لحاجاته الشّخصية أو المهنية، أمّا الاتجاه الثاني الضيق فقصد به كل شخص يتعاقد لأجل اشباع حاجاته الشّخصية أو العائلية غير المرتبطة بنشاطه المهني.[107] وأيّدت غالبية الفقه الفرنسي هذا المفهوم الضيق للمستهلك.

كما وإنّ التعريف القانوني للمستهلك بموجب قوانين حماية المستهلك في المملكة المتحدة والاتحاد الأوروبي هو شخص طبيعي يتصرّف خارج نطاقه المهني.[108]

تزداد صعوبة تمييز ما هو خاص وما هو مهني بزيادة استخدام الأشخاص للانترنت وخاصةً الحوسبة السّحابية.

غالباً ما يكون غير واضح إذا كان المستهلك يستخدم الخدمة كمستهلك أو لمهنة أو حرفة، أو مزيج غير مؤكد من الاثنين. حتى إذا لم يتم تسويق الخدمة السّحابية على المستوى الإحترافي، فيمكن استخدامها على الصّعيد المهني بكل سهولة؛ وتصعب المسألة إذا كانت الإدارة السّحابية بيد المستهلك نفسه، وربما أقل إذا كانت نيابة عنه من إدارة ثابتة أو رسمية مرتبطة بمهنته.

من الأمثلة على هذه الصّعوبة في التصنيف هو استخدام الخدمات السّحابية المجانية مثل Gmail وFacebook للدعاية والإعلان عن الشّركات الصّغيرة وجديدة النشأة. فقبل تطوير هذه الخدمات، كانت تكاليف الإعلانات والتسويق والبريد الإلكتروني باهظة. الآن يتم توفير هذه الخدمات مجاناً، ببساطة مقابل إضافة قيمة إلى شبكة إجتماعية أو نظام أساسي عبر الانترنت. فهي تُستَخدَم لأغراض شخصية وأغراض تجارية ومهنية على حد سواء وخاصة من قبل الشّركات التجارية جديدة النشأة لأنها لا تتطلب أي رأسمال استثماري. فيمكن إعداد حساب Gmail بسرعة وسهولة ليتم استخدامه من قبل شخص يرغب في التواصل مع العملاء ولكن يمكنه أيضاً استخدامه للبريد الالكتروني الشخصي وبالعكس يمكن استخدام حساب Gmail موجود لحاجات مهنية.

كما أن Facebook هي طريقة مجانية وموثوقة للإعلانات التجارية وقد يكون الحساب منشأ قبل الإعلان أو بهدف الإعلان.

هذه التطورات الإجتماعية والإقتصادية والتكنولوجية تتحدى بوضوح التعريفات التي سبق وذكرناها.

فالمشكلة الأساسية المطروحة هي إذا ما كان القانون يحمي هذا النوع من التعاقد، أو متى يحميها؟

يجب الأخذ بنية المتعاقد عند إبرام العقد وصفة دخوله الأساسية، فإذا تم ذلك كمستهلك لا يهم إذا قرر لاحقاً استخدام الخدمة لأغراض مهنية. إلّا أنه في حالة السّحابة يصعب معرفة نيته عند التعاقد إذ في

---

107 Gestin: "**Traite’ de droit civil, les obligations, les contrats, formation**", Adition Pris L.G.D.G, 1988, page 46, no. 59.

108 Supra 72, page 778.

أغلب الأوقات لا معرفة بين الطرفين وليس هناك من رقابة من قبل المزوّد على البيانات الموضوعة على السّحابة. والأصعب هو معرفة تاريخ أو وقت تغيير استعماله للخدمة. لكن يجب أن يتمتع المستخدم في جميع الحالات بحماية إذ إنّه الطرف الضعيف في العلاقة مهما كانت استخداماته للسّحابة. يمكن تصنيف الضعف إمّا بالضعف الشّخصي أو الضعف النسبي أو ضعف المعرفة.

1. الضعف الشّخصي أو الضعف المرتبط بالشّخص

يرتبط هذا النوع من الضعف بشخص المتعاقد نفسه، نابعاً منه، عندما تكون معرفته ودرايته بموضوع العقد لا ترتقي إلى المستوى الذي يجعله يتخذ موقفاً أو قراراً يعبّر عن رضا مستنير في ما يخص الإلتزامات والحقوق المتبادلة في العقد.[109]

في القواعد العامة هناك تطبيقان أساسيان لهذا النوع، الأول يتضمن حالات انعدام التمييز أو نقصانه لدى المتعاقد، والثاني يشمل حالات تعيّب الإدارة أو اضطراب التمييز لسبب عارض ومع ذلك فقد يكون العاقد بالغاً رشيداً إلّا أنه يعدّ طرفاً ضعيفاً في بعض الأحوال، وذلك عندما لا يكون على علم بالنظام القانوني الذي يخضع له العقد أو أنه يجهل بعض الظروف والملابسات المتعلقة بموضوعه.[110]

2. الضعف النسبي

قد يتمتع المتعاقد بالأهلية اللّازمة لإبرام العقد، إلّا أن رضاه قد يكون مشوباً بعيب ما، فيكون مميزاً أو مدركاً لما يلتزم به، ومع ذلك فهو يعتبر طرفاً ضعيفاً إذ يضطر إلى قبول شروط تعسفية مفروضة من قبل المتعاقد الآخر، دون أن يمتلك الإرادة الحرّة للاختيار بين قبول هذه الشّروط أو رفضها، وهو ما يطلق عليه الضعف النسبي أو الضعف الإقتصادي.[111]

---

[109] Fontaine (M): "**La protection de la partie faible dans les rapports contractuels**", Rapport de synthèse, comparaisons Franco-Belges, L.G.D.J., 1996, Page 615.

[110] علاء عمر محمد الجاف، **الآليات القانونية لحماية المستهلك في عقود التجارة الإلكترونية (دراسة مقارنة)**، منشورات الحلبي الحقوقية، بيروت، الطبعة الأولى، 2017، ص. 72.

[111] Delvaux (P.H): "**Les contrats d'adhésion et les clauses abusives en droit belge, en la protection de la partie faible dans les rapports contractuels (comparaisons franco-belges)**", L.G.D.J., 1996, PAGE 73.

3. الضعف في المعرفة

يتكون هذا النوع من الضعف عند إبرام عقد بين طرفين، تنعدم المساواة بينهما على صعيد المعرفة والخبرة، فيكون جاهلاً لمعلومات أو بيانات، أو تنقصه خبرة شخصية أو عملية تتعلق بإبرام العقد يملكها العاقد الآخر؛ لذلك لا يكون التفاوت بينهما تفاوتاً اقتصادياً وإنما تفاوتاً في العلم أو المعرفة.[112]

تطبيقاً على عقود الحوسبة السّحابية، قد تجتمع هذه الأنواع الثلاثة من الضعف في شخص المستهلك، إذ إن المستهلكين يفتقرون المعرفة والثقافة في هذا الموضوع بشكل عام، كذلك يتمتع مزوّد الخدمة بالقوة الاقتصادية ويفرض شروط العقد على الطرف الثاني، بالإضافة إلى افتقار معرفته بالنظام القانوني للعقد، وجميعها في أغلب الأحيان تتواجد في المستهلك الواحد عند إبرامه للعقد، لهذا السّبب تزداد ضرورة حمايته أهميّة.

النبذة الثانية: الحماية المسبقة واللّاحقة للمستهلك

لكل علاقة تعاقدية مرحلتان سابقة ولاحقة لإبرام العقد، وكلٌّ من هاتين المرحلتين قد توقع المستهلك بحالات حرجة توجب الحماية.

البند الأول: الحماية المسبقة للمستهلك

يتم أولاً الإعلان أو العرض على شبكة الانترنت سواء على صفحات الويب أو بواسطة مجالس النقاش أو ندوات الاتصال أو البريد الالكتروني. وبالنسبة لهذا الأخير، تم تكريس نظامين، نظام الـ OPT–OUT الذي يفرض على المستهلك الاعتراض على الاتصالات الالكترونية غير المرغوب فيها بعد بلوغها إليه. وقد تبنى قسم من الدول النظام الأول وقسم آخر النظام الثاني فمثلاً فرنسا تبنت لـOPT–OUT في المادة L121–20–5 من قانون الاستهلاك، كذلك القانون اللّبناني 2018/81 نصّ في المادة 32 منه: "... يجب أن تتضمن كل رسالة ترويج أو رسالة تسويق، تحديد للعنوان الذي يمكن للمرسل إليه أن يرسل عليه طلباً يرمي إلى وقف هذا النوع من الرسائل نهائياً دون تكبد أية مصاريف."

والخطورة التي يجب حماية المستهلك منها هي الإعلان الخادع، وقد نص عنها قانون حماية المستهلك اللّبناني رقم 2005/659 ذات الاتجاه العام أي أنها قابلة للتطبيق على شبكة الانترنت.

لقد نصّت المادة 11 من القانون المذكور الإعلان "الذي يتم بأيّة وسيلة كانت" ويتناول سلعة أو خدمة ويتضمن عرضاً أو بياناً أو ادعاء كاذباً، أو أنه مصاغ "بعبارات من شأنها أن تؤدي، بطريقة

---

[112] د. حسن عبد الباسط جميعي، **أثر عدم التكافؤ بين المتعاقدين على شروط العقد**، دار النهضة العربية، القاهرة، 1991، ص. 101.

مباشرة أو غير مباشرة إلى خداع أو تضليل. واعتبرت في فقرتها الثانية أنه يعتبر كاذباً أو مضللاً عندما يتناول مثلاً طبيعة السّلعة أو تركيبتها أو صفاتها الجوهرية.

يعاقب الخادع بالحبس من شهر إلى ثلاثة أشهر وبغرامة من عشرة ملايين إلى خمسين مليون ليرة لبنانية أو بإحدى هاتين العقوبتين إستناداً إلى قانون 2018/81.

كما تضمن قانون المعاملات الإلكترونية والبيانات ذات الطابع الشّخصي اللّبناني الصّادر تحت رقم 81 بتاريخ 2018/10/18 أنه يجب الإشارة إلى أن الإعلان دعائي ويجب أن يتضمن تعريفاً بالشّخص الذي يتم الإعلان لصالحه.[113] وهذه حماية إضافية للمستهلك تجنبه الوقوع في الخطأ.

بالإضافة إلى أن الإعلان قد يشكل إيجاباً في حال تضمن جميع المسائل الجوهرية لإنشاء العقد كوصف السّلعة أو الخدمة، وبيان صفاتها الأساسية والثمن، شروط البيع، الإجراءات الواجب اتباعها لطلب السّلعة أو الخدمة. لقد نصّ قانون رقم 2018/81 في المادة 31 أنه على كل من يمارس التجارة الإلكترونية أن يؤمن للأشخاص الذين يتعامل معهم ولوجاً سهلاً ومباشراً ودائماً إلى المعلومات الآتية:

1. اسمه وشهرته ومحل إقامته، إذا كان هذا الشّخص طبيعياً.
2. اسمه واسم ممثله القانوني ومركزه وعنوانه التجاري، إذا كان شخصاً معنوياً.
3. العنوان المفصل لمحل إقامة الشّخص وعنوان بريده الإلكتروني وعنوان الموقع الإلكتروني المستعمل وأرقام الهاتف أو أية وسيلة إتصال أخرى.
4. رقم ومكان تسجيله في السّجل التجاري ولدى الدائرة الضريبية المختصة.
5. صفته المهنية والإشارة إلى القواعد المهنية المطبقة عليه، إذا كان عضواً في مهنة منظمة أو نقابة.
6. بياناً تفصيلياً بالثمن أو البدل مبيناً جميع الضرائب والرسوم والنفقات الإضافية المستحقة.

كما ويجب أن يشمل عرض التعاقد في العقود عن بعد على:

1. طبيعة المنتج أو الخدمة المعروضة وكيفية استعمالها وأخطارها.
2. ثمن المنتجات والخدمات وملحقاتها، كالضرائب أو أية أعباء أخرى محتملة وزمان ومكان وطريقة الدفع.
3. كفالات ما بعد البيع، اللّاحقة للعقد، التي عرضها المحترف.
4. تاريخ تسليم المنتج، أو تنفيذ الخدمة، ومكانه، والنفقات عن ذلك.
5. تحديد مهلة قبول العرض إذا كان محدداً بمدة معينة.[114]

---

[113] المادة 32 الفقرة الأولى من القانون 2018/81: "يجب أن يتضمن كل إعلان دعائي يمكن الولوج إليه على الخط بأية وسيلة من وسائل الاتصال الالكترونية، الإشارة إلى أنه إعلان دعائي، كما يجب أن يتضمن تعريفاً بالشّخص الذي يتم الاعلان لصالحه."

[114] المادة 52 من قانون 2005/659.

وفي هذا الإطار تجدر الإشارة بصورة خاصة إلى ما أوردته المادة 53 من قانون 2005/659 التي فرضت في التعاقد على الانترنت تزويد المستهلك: مستند يتضمن كافة المعلومات المنصوص عليها في المادة 52 لتمكينه من اتخاذ قراره بالتعاقد.

وبذلك يلتقي قانون حماية المستهلك اللّبناني بالتشريعات الفرنسية والأوروبية كما والعربية.[115]

البند الثاني: الحماية اللّاحقة للمستهلك

1. الحق في التفكير

عند إعطاء المستهلك البيانات والعقود لمراجعتها يجب أن يعطى أيضاً مهلة للتفكير وهذا ما يعرف بحق التفكير، إذ لا جدوى من تزويده بالبيانات بنيّة حمايته دون منحه فرصة للتفكير. ففرض المشرع شروط تسليم المستهلك نسخة عن العقد أو يضع العقد بطريقة يمكن للمستهلك الوصول إليها للإطلاع على شروطه قبل توقيعه[116]، كي يصدر قراره عن روّية وتبصّر.

بالإضافة إلى حقه بالعدول عن قراره بشراء السّلعة أو استئجارها أو الاستفادة من الخدمة التي نصّت عنه المادة L.121-20 من قانون الاستهلاك الفرنسي وكذلك المادة 129 من قانون رقم 2018/81 التي ألغت بموجبها المادة 55 من القانون رقم 2005/659 واستعاضت عنها بالنص المذكور في هذه المادة[117]، وذلك خلال مهلة 10 أيام من تاريخ التعاقد إلّا إذا اتفق الطرفان على مدّة أطول يستفيد منها المستهلك.

2. وقت ابرام العقد

يُبرم عقد البيع الإلكتروني عند إلتقاء الإيجاب بالقبول، وانقسمت القوانين حول الأخذ بمذهب إعلان القبول ومذهب العلم أي عند علم البائع أو مقدم الخدمة بقبول المستهلك إلّا أن المشرع اللّبناني وقبله

---

[115] فريد منعم جبور، **حماية المستهلك عبر الانترنت ومكافحة الجرائم الإلكترونية (دراسة مقارنية)**، منشورات الحلبي الحقوقية، بيروت، الطبعة الثانية، 2012، ص. 24-25.

[116] المادة 20 والمادة 54 من قانون حماية المستهلك رقم 2005/659.

[117] المادة 129 من قانون 2018/81: "يلغى نص المادة 55 من قانون حماية المستهلك رقم 659 تاريخ 2005/2/4 ويتعاض عنه بالنص التالي:

خلافاً لأي نص آخر، يجوز للمستهلك، الذي يتعاقد وفقاً لأحكام هذا الفصل، العدول عن قراره بشراء سلعة أو استئجارها أو الاستفادة من الخدمة وذلك خلال مهلة عشرة أيام تسري اعتباراً اما من تاريخ التعاقد في ما يتعلق بالخدمات، او من تاريخ التسليم في ما يتعلق بالسّلع. الا انه في حال الاتفاق على مهلة اطول في العقد فتعتمد عندئذ المهلة المذكورة في العقد.

الفقه اللّبناني أتى واضحاً بأخذه بمذهب العلم في المادة 38[118] معطوفاً على المادة 35 من قانون 2018/81 إذ يلزم مقدم العرض إبلاغ الطرف الآخر بورود القبول تحت طائلة التعويض إذا ما أخلّ بهذا الموجب.[119]

3. دفع الثمن

المشرع اللّبناني لم يمنع الدفع قبل انقضاء مهلة العدول، وإنما في حال مارس حقه في العدول، فرض على المحترف إعادة المبالغ التي يكون قد تقاضاها، على أن يتحمل المستهلك، عند العدول بعد التسليم أو الاستفادة من الخدمة، مصاريف وأتعاب التسليم أو تزويد الخدمة.

وقد جاء القانون اللّبناني منسجماً مع أحكام الإرشاد الأوروبي المتعلق بالعقود عن بعد، مجيزاً الدفع المسبق قبل نهاية مهلة العدول: والمشترع اللّبناني في هذا الخصوص أقل حمايةً للمستهلك من القانون الفرنسي الذي لا يجيز استيفاء الثمن قبل انتهاء المهلة.[120]

4. في المنازعات

في أغلب الأحيان تنص هذه العقود على الطرق البديلة لحل النزاعات أي غير قضاء الدولة، لما لها من حسنات، وأنواعها عديدة كالوساطة (mediation) والمصالحة (conciliation) والتحكيم (arbitrage). ولكن هذه الطرق لا تلغي قضاء الدولة، فنرى الكثير من مقدمي الخدمات نصوا على اختصاص محاكم دول محددة مع القوانين الواجبة التطبيق بالإضافة إلى الطرق البديلة، فيعطى المستهلك الخيار بالوسيلة التي تناسبه أكثر، وهذه تعتبر حمايةً له، وسنتكلم مفصلاً عن طرق حل المنازعات في الفقرات القادمة.

5. حماية بياناته الشّخصية

البيانات ذات الطابع الشخصي هي جميع أنواع المعلومات المتعلقة بشخص طبيعي التي تمكّن من التعريف به، على نحو مباشر او غير مباشر، بما في ذلك عن طريق مقارنة المعلومات المتعددة

---

[118] المادة 38 الفقرة الأولى من قانون 2018/81: "عندما يصدر القبول بالوسيلة الإلكترونية في العقود المدنية والتجارية، لا يعتبر هذا القبول منشئاً للعقد إلّا بعد أن يؤكد عليه مرّة ثانية من وجه إليه العرض بعد أن يكون قد تحقق من مضمون التزامات الفريقين."

[119] المادة 35 من قانون 2018/81: "على مقدم العرض إبلاغ الطرف الآخر بورود القبول وذلك ضمن مهلة معقولة أو ضمن المهلة الزمنية المحددة في العرض.يلزم مقدم العرض بالتعويض عن أي إخلال بهذا الموجب ينشأ عنه ضرر."

[120] فريد منعم جبور، مرجع سابق، ص. 57.

المصادر أو التقاطع في ما بينها.[121] فجاء القانون رقم 2018/81 الذي يتعلق بالمعاملات الالكترونية والبيانات ذات الطابع الشّخصي يحتوي على نصوص تتلاءم مع متطلبات عصر المعلوماتية خاصةً بما يوفره من حماية للبيانات الشّخصية في مواجهة مخاطر المعالجة[122] الآلية، لاسيّما وأنه جاء متطوراً ومستفيداً من الانجازات الأوروبية (القانون الفرنسي المتعلق بالمعلوماتية والحريات لعام 1987م والقانون الفرنسي رقم 2004/801 الصّادر في 6 آب 2004 المعدل لأحكام القانون المذكور سابقاً)، والنظام القانوني الأوروبي (الإرشاد الأوروبي رقم 95/46 الصّادر بتاريخ 24 تشرين الأول 1995 المتعلق بحماية الأشخاص الطبيعيين إزاء معالجة البيانات ذات الطابع الشّخصي)، فجاء الباب الخامس من القانون 2018/81 ينص عل حماية البيانات ذات الطابع الشّخصي وطريقة تجميعها ومعالجتها إذ يجب أن تكون بأمانة ولأهداف مشروعة ومحددة وصريحة، ولزيادة الحماية نصّ الفصل الخامس من هذا الباب على أحكام جزائية تطبق عند الإخلال بأي من الشّروط التي نُصَّ عليها فيه.

[121] المادة الأولى من القانون رقم 2018/81.

[122] المعالجة هي كل عملية او مجموعة عمليات تقع على هذه البيانات مهما كانت الوسيلة المستخدمة، لا سيما عمليات التجميع والتسجيل والتنظيم والحفظ والتكييف والتعديل والاقتطاع والقراءة والاستعمال والنقل والنسخ والنشر والمحو والاتلاف وكل شكل آخر لوضع المعلومات تحت التصرف.

القسم الثاني: المخاطر والعوائق التي تواجه الحوسبة السّحابية

بعد تعريف الحوسبة السّحابية ومقاربتها مع غيرها من العقود والخدمات والتكلم عن أهميتها، يجب التطرق إلى المخاطر والعوائق التي تواجه الشّخص عند استعماله لهذه التكنولوجيا كما والحلول القانونية والتقنية التي يمكن أن يلجأ إليها عند اعتراضه لأية مشاكل. هذه المخاطر يمكن تقسيمها إلى مخاطر تقنية وأخرى قانونية؛ يجب عند إختيار المزوّد أن يتمتع بثقة الجمهور أي أن يتمتع بسمعة ومصداقية وشفافية. في هذه الخدمة يجب أن يحرص على سلامة الشّبكة وعلى ألّا يقوم بحذف البيانات وفك التشفير أي ألّا يدخل إلى البيانات المؤمّن عليها أو المحفوظة لديه بدون تصريح المستخدم كما عليه أن يعمل على صيانة الخوادم لديه لكي يتمكن المستخدم من استعمالها والإستفادة منها في أيِّ وقت يريد، وهي ميزة أساسية لهذه الخدمة. البيانات المحفوظة في الخوادم يجب أن تؤمّن سريّتها ولكن ما هي البيانات التي تتطلب الأمان والسّرية؟ هل هي كل معلومة يمكن الوصول إليها؟ وما هي المخاطر التي يمكن أن تواجه السّرية؟ أي كيف يمكن للجهات الثالثة الحصول عليها؟ وما دور المزوّد في مثل هذه الحالات؟ وأخيراً سوف نتعمق في البيانات ذات الطابع الشّخصي والحق في الخصوصية التي هي أكثر البيانات المتطلبة حماية والحقوق القانونية التي يتمتع بها المستخدم عند تواجده في السّحابة.

الفصل الأول: المخاطر التقنية

المخاطر التقنية تؤثر سلباً على المستخدم وعلى الشّركة على حدّ سواء، فليس من صالح الشّركة أن تهمل الحماية والإعتناء الدقيق في الشّق التقني الذي تقدّمه فتخسر عملاءها وتتأثر سمعتها في السّوق وبين مثيلاتها. تسعى الشّركات إلى إكتساب ثقة المستخدمين عبر الشّفافية في وصفها سياسة الشّركة وكيفية عملها والتقديمات التي توفرها والشّفافية في التطبيق. ففي هذا الفصل سنتطرق إلى المخاطر التقنية وما يجب على الشّركات القيام به لمواجهتها.

المبحث الأول: الثقة في المزوّد

من الشّروط الأساسية التي يجب أن يتمتع بها المزوّد قبل إختياره من ضمن العديد من المزوّدين هي الثقة، ثقة الجمهور. فعند إختيار العميل لهذه الشّركة أو تلك، يبحث عن رأي عملائها بها خاصةً ثقتهم بها، إذ إن المستخدم يعطي المزوّد ثقته عند نقل بياناته إلى خوادم هذه الشّركة وثقته بأنهم لن يدخلوا إليها أو يعدلوا عليها. فما هي الأمور التي تؤدي إلى اضطراب ثقة المستخدم بالشّركة المختارة؟ سنرى في هذه الفقرة التعديل غير المصرّح به، التشفير وحذف البيانات.

الفقرة الأولى: حالة الشّبكة والحذف

يجب على مزوّد الخدمة العمل على أن تكون الشّبكة التي تعبر من خلالها البيانات التي تصل إلى سحابته آمنة من دون أي إعتراض، كما ويجب عليه العمل على زيادة مصداقيته وشفافيته في العمل.

النبذة الأولى: تعديل غير مصرّح

من أكبر المخاوف المتعلقة بحفظ البيانات في السّحابة هو التحقق من سلامة البيانات في الخوادم غير الموثوقة وكيفية التعامل مع البيانات الحساسة، فقد تعاني هذه البيانات من التلف عند الإرسال من/إلى التخزين. بما أنه يتم إرسالها إلى خوادم بعيدة، يجب الحفاظ على سلامة البيانات والتحقق منها باستمرار لإثبات أن البيانات والحسابات سليمة. فيجب حمايتها من أيّ تعديل غير مصرّح به وهذا ما يسمى بالـ Data Integrity [123] أي تكامل البيانات. ولتبسيط مفهوم Data Integrity، يمكن تعريفه على أنه ضمان أن البيانات غير متغيّرة وصحيحة. يمكن إعاقة سلامة البيانات في أي مستوى من مستويات التخزين، لهذا السّبب تعتبر مراقبة نزاهة التخزين هي المشكلة الأكثر أهمية لأي مركز بيانات. ومن الأمثلة التي قد تؤدي إلى فقدان النزاهة في التخزين: bit rot أي تلف البيانات أو وسائط التخزين، فشل وحدة التحكم، فساد البيانات الوصفية، الازدواجية وفشل الشّريط. ولكن تعد الـ bit rot الأكثر أهمية إذ هو التلف أو الفساد البطيء في أداء وسلامة البيانات المخزنة على وسائط التخزين. وهو معروف أيضاً بـ Data Rot أي تلف البيانات، Data Decay أي تآكل البيانات و Silent Corruption أي الفساد الصّامت. وسبب آخر لفساد البيانات يمكن أن يكون الترحيل أو النقل إلى خوادم أو منصات مختلفة.[124]

يمكننا أخذ مثال (Google App Engine (GAE تتضمن الكثير من المراحل التي من خلالها المستخدم يطلب الانتقال إلى السّحابة. والضعف في هذا المثل يكمن في أنه عندما يريد المستخدم استرداد بعض البيانات يرسل طلباً لمزوّد الخدمة كذلك عندما يرغب في تخزين بعض منها يرسل طلباً

[123] Suttan Aldossary & William Allen: "**Data Security, Privacy, Availability and Integrity in Cloud Computing: Issues and Current Solutions**", article published in International Journal of Advanced Computer Science and Applications, Vol. 7, No. 4, 2016, page 489.

[124] Raj Kumar Chalse, Ashwin Selokar & Arun Katara: "**A New Technique of Data Integrity for Analysis of the Cloud Computing Security**", CICN 2013, pp. 469-472.

ولكن في الوقت عينه يتم إرسال MD5sum [125] أو SHAsum [126] معه. فعندما يتلقى مزوّد الخدمة الطلب يحفظها تحت رقم التشفير. ولكن من وجهة نظر المزوّد لا يكفي الحفاظ على سلامة البيانات عند التحميل والتنزيل ولكن أيضاً خلال مرحلة التخزين. فهناك تقنيات متنوّعة تم تطويرها مثل استخدام مدقق خارجي موثوق به أو تشفير كامل قاعدة البيانات مثلاً كالحفاظ على سلامة البيانات أثناء الإرسال بواسطة SSL Channel [127]. ولكن لسوء الحظ هذا الإجراء لا يضمن عدم تعديل البيانات في مساحة التخزين.

وفي هذا المثال تثار ثلاثة مخاوف مهمّة:

1. السّرية: بالرغم من أن مزوِّد السّحابة (X) لديه حق الوصول الكامل إلى جميع بيانات المستخدمين (Z & Y)، فإنّ (X) يعتبر غير موثوق به ف (Y) و(Z) لا يريدان كشف بياناتهما.
2. النزاهة: كون (X) المسؤول، فلديه القدرة الكاملة للتصرف بالبيانات وتعديلها، إذا كان (Y) يحاول استرداد بعض البيانات التي تم إرسالها بواسطة (Z) أو التي تم تعديلها من قبل (X).
3. الرفض: في حال اكتشف (Y) أن البيانات قد تم التلاعب بها أو تعديلها، هل هناك أي دليل على إثبات أن (X) مذنب؟ وبالمثل، يحتاج (X) إلى بعض الأدلة للدفاع عن نفسه وإثبات براءته.[128]

هل هذا التلاعب أو التعديل يشكل جريمة أم مجرد ضرر؟ يجب التمييز بين عدّة حالات:

- إذا كان التعديل نتيجة إنتقال البيانات إلى الخادم بدون أي فعل بشري، لا يرتب الأمر أية مسؤولية على مقدم الخدمة، ولكن يجب الإشارة إلى أن هذا التعديل من النادر جداً أن يحدث حالياً مع التطور في هذا المجال.
- إذا كان التعديل نتيجة تدخل بشري، يجب التمييز بين حالتين أيضاً:
- إذا كان الفاعل مقدم الخدمة وثبت هذا الأمر، فتكون جريمة الولوج غير المصرح به إلى البيانات؛ أمّا إذا كان التعديل بفعل شخص ثالث، فيكون هذا الأخير قد إرتكب جريمة بحق صاحب البيانات،

---

[125] MD5 اختصار لـ MD5 Message-Digest Algorithm هي طريقة تشفير، الغرض الرئيسي منها التحقق من أن الملف لم يتم تعديله، وبالتالي يعتبر بصمة التطبيق. MD5sum هو تطبيق حوسبة يستخدم للتحقق من سلامة الملفات ومطابقة الملف المنزل على الحاسوب مع الملف الأصلي حيث أن أي تغيير في الملف سيؤدي إلى تغيير تجزئة MD5.

[126] SHA اختصار لـ Secure Hash Algorithm وهي كـ MD5 وسيلة تشفير. كذلك الـ SHAsum له نفس وظيفة الـ MD5sum.

[127] SSL توفر قناة آمنة بين جهازين أو أكثر تعمل عبر الانترنت أو شبكة داخلية، عند إرسال البيانات أو نشرها من خلال متصفح يستخدم HTTPS، تضمن أن هذه المعلومات مشفّرة وآمنة من أي إعتراض.

[128] Siddharla Rao, Savan Gujrathi, Mithun Sanghui & Shubham Shah: "**Analysis on Data Integrity in Cloud Environment**", OSR Journal of Computer Engineering e-ISSN: 2278-0661, p-ISSN: 2278-8727, Volume 16, Issue 5, Ver. IX (Sept-Oct. 2014), PP 71-76.

أمّا مزوِّد الخدمة يكون مسؤولاً عن الضرر الحاصل إذا كانت هذه الجريمة قد إرتكبت بسبب إهماله أو عدم تنفيذه للموجبات المترتبة عليه.

- إن الجريمة تكون محققة بحق مرتكبها إذا كان هناك نص يجرمها إذ لا جريمة بدون نص[129]، كذلك إذا تحقق الركنان المادي والمعنوي، فالركن المادي هو الذي تظهر فيه الجريمة إلى الخارج وتتجسد، أي النتيجة؛ والركن المعنوي هو قصد الفاعل بارتكاب هذا الفعل لتحقيق النتيجة التي حصلت وعليه تكون الجريمة مقصودة. أمّا الجريمة غير المقصودة فتترتب بسبب إهمال أو قلّة إحتراز أو عدم إحترام الأنظمة والقوانين؛ وليس هناك من درجة معينة للخطأ الجزائي لقيام المسؤولية الجزائية.[130] وبالتالي في جميع الحالات التي سبق ذكرها، نكون أمام مسؤولية جزائية بالإضافة إلى المسؤولية التعاقدية التي تترتب على مزوّد الخدمة إذا كان يتوجب عليه القيام بموجب منصوص عليه في العقد.

وعليه، يتطلب ضمان سلامة البيانات وجود ثقة بين العميل والمزوّد، وبعض الأساليب التي تعزز ضمان سلامة بيانات العميل وهي:

- فحص الدلالة
- شهادة معتمدة من وكالات موثوقة
- قناة موثوقة أي ضمان أن البيانات تنتقل عبر قناة مصرح بها
- استخدام وسيلة تشفير البيانات
- البنية التحتية الأفضل للمشاريع إذ يجب على البنية التحتية للشركات أن تكون قادرة على كبح الهجمات السّيبرانية
- أنظمة الاسترداد الجيّدة في حال حدوث أيّ ضرر للبيانات أو فقدانها
- وثائق العقد بين الطرفين جيّدة وواضحة.[131]

النبذة الثانية: التشفير وحذف البيانات

للتشفير عادةً فوائد كثيرة، هدفها الرئيسي حماية بيانات المستهلك وزيادة الأمان عليها؛ لكن بالرغم من استخدامها للحماية إلّا إنه هناك العديد من مستويات التشفير وأنواع تشفير قد تؤدي إلى إشكاليات؛

---

[129] المادة الأولى من قانون العقوبات اللّبناني.

[130] سمير عاليه وهيثم سمير عاليه، **الوسيط في شرح قانون العقوبات "القسم العام"**، المؤسسة الجامعية للدراسات والنشر والتوزيع، الطبعة الأولى، بيروت، 2010، ص. 238-311.

[131] Pradeep Kumar Tiwari & Dri Bharat Mishra: "**Cloud Computing Security Issues, Challenges and Solutions**", IJETAE August, 2012, Vol. 2 Issue 8, pp. 306-309.

كما يمكن أن يكون هناك أساليب تمكّن المزوّد الوصول إلى بيانات مشفرّة وهنا يكمن عامل الثقة في المزوّد وسمعته. هذه القدرة على الحصول على البيانات قد تؤدي إلى حذف البيانات، أو حتى في نهاية الخدمة يجب أن يحصل حذف للبيانات، إذ إن المستخدم قد يثق بمزوّد ما علماً منه أنه سيقوم بحذف البيانات عن جميع خوادمه عند انتهاء العقد أو مدّة الخدمة.

البند الأول: التشفير

يمكن منع الوصول غير المصرّح به أو الحد من قبل المستخدمين الذين يقومون بتشفير بياناتهم بإحكام قبل التحميل في السّحابة. قد تعمل تطبيقات التشفير على تحويل مجموعة بيانات كاملة من خلال تطبيق "algorithm" أو "الخوارزمية" عليها. على سبيل المثال، ترجمة المعلومات إلى لغة أخرى بحيث لا يتمكن سوى الأشخاص الذين يعرفون تلك اللّغة من فهم الترجمة، وبالمثل البيانات المشفرة مصممة للاستخدام فقط من قبل الشّخص الذي لديه مفتاح فك التشفير ويمكنه استعماله. يقوم التشفير أحادي الاتجاه بتطبيق وظائف الاتجاه الواحد (cryptographic hash functions) [132] على البيانات مما ينتج عنه أجزاء ذات طول ثابت من المفترض أن يكون غير قابل للإلغاء فمثلاً كلمات المرور تكون غالباً جزءاً أحادي الاتجاه. بينما التشفير المتبادل (two–way cryptography) قابل للانعكاس، مما يسمح بإعادة تشكيل مجموعة البيانات الأصلية (فك التشفير) ولكن فقط من قبل أشخاص معينين، أو في ظروف معيّنة. وبالتالي يمكن استخدام التشفير لتأمين السّريّة.

العوامل التي تؤثر على أمان البيانات المشفرة ضد فك التشفير غير المصرّح به تشمل: قوّة أسلوب التشفير (قوة التشفير الخوارزمية)، طول مفتاح التشفير (المفاتيح الأطول أكثر أماناً بوجه عام ضد الهجمات)، وإدارة المفاتيح بما في ذلك تخزين فك التشفير، والأمان والتحكم في الوصول إلى المفاتيح.[133] ولكن قد يتم كسر (break) أو تشقق (crack) بعض طرق التشفير.

يمكن تطبيق التشفير على البيانات داخل ملف إلكتروني أو مجلّد أو قاعدة بيانات أو مجموعة أخرى من المعلومات. يمكن للمستخدمين تطبيق التشفير على أجزاء، أو على نحو أكثر شيوعاً، على كل مجموعة بيانات أو قاعدة بيانات قبل تخزينها في السّحابة. على سبيل المثال، قد يتم تطبيق التشفير

---

[132] تقنية Hashing تختلف عن encryption، فهي وسيلة لحفظ البيانات بشكل غير قابل للاسترجاع أبداً وبالتالي الفرق كبير بينهم وبين تطبيقاتهم فالتشفير يمكن فكه واسترجاع البيانات بينما الـ Hashing لا يمكن على الإطلاق بالرغم من أن الكثير من الأحيان تستخدم hashing algorithms كطريقة للتشفير.

[133] Matt Blaze et al.: "**Minimal Key Lengths for Symmetric Ciphers to Provide Adequate Commercial Security**", US Defense Technical Information Center, 1996. (Available on: https:www.dtic.mil/cgi-bin/GetRDoc?AD=ADA389646) (Accessed on 15 September 2018, at 10:05 AM).

أحادي الإتجاه أو ثنائي الإتجاه فقط على الأسماء، ولكن البيانات الأخرى تبقى قابلة للقراءة كـ "نص عادي". بالمقابل، يمكن تطبيق تشفير ثنائي الاتجاه على مجموعة بيانات كاملة قبل التخزين للاستخدام في المستقبل. يمكن تطبيق التشفير داخل جهاز كمبيوتر المستخدم قبل الإرسال، باستخدام برنامج خاص به، أو مقدم خدمة. حتى عندما يرسل المستخدمون بيانات غير مشفرة إلى السّحابة، قد يقوم المزوّدون بتشفير كل البيانات المتلقاة أو جزء منها من أجل تخزين البيانات بطريقة أكثر أماناً أو قبل استخدام أو بيع بيانات شخصية مجهولة المصدر أو مستعارة. يؤدي فك التشفير وإعادة التشفير إلى تدني مستوى أداء الخدمة وهذا أحد عيوب التشفير. علاوة على ذلك، حتى البيانات المشفرة بشدّة إلى الدرجة الأمنية يجب أولاً فك التشفير فيها (حتى إذا تم إعادة تشفيرها بعد ذلك) لتمكين التطبيقات من معالجة البيانات بشكل جيّد مثل الفرز أو التحليل أو الفهرسة.[134]

قد تكون البيانات الموجودة في "مسح" وغير مشفرة عرضة لوصول مقدمي الخدمات أو أطراف ثالثة. والطريقة الوحيدة لتجنب هذه الثغرة الأمنية هي تنزيل البيانات المشفرة إلى أنظمة المستخدم الخاصة ثم فك تشفيرها محلياً.

إن استخدام بيانات غير مشفرة يسمح بالوصول غير المصرح به إذا تمكن المتسللون من الوصول إلى البيانات الموجودة على أنظمة المزوّدين، لذلك تعتبر أنظمة منع التطفل والكشف كالجدران النارية مهمة. تم تصميم العديد من الأنظمة لمنح مقدمي الخدمات "backdoors"، وهي تقنية تمكن من الوصول إلى بيانات المستخدم (على الأقل غير المشفرة منها) حيث أن المزوّدين قد يحتاجون إلى الوصول لأغراض الصّيانة. في مثل هذه الحالات، تتطلب زيادة السّرية فرض قيود على التحكم في الوصول: تقليل فئة (فئات) الموظفين الذين لديهم وصول تقني وتقييد وصولهم أو الاستخدامهم أو الإفصاح عن البيانات التي تم الحصول عليها من خلال العقد مثلاً بما في ذلك فرض التزامات السّرية الملزمة قانوناً.[135]

كذلك يجب على المستخدمين الذين يتحكمون في وصول موظفيهم إلى بيانات السّحابة الخاصة بهم إدارة هذا الوصول بشكل صحيح، وذلك لمنع الموظفين من إساءة استخدام أو الإفصاح عن مثل هذه البيانات بدون تفويض ومن المرغوب وجود أساليب قويّة للتوثيق في كلتا الحالتين.

كما وإن الوصول غير المصرّح به ممكن إذا تم اعتراض البيانات أثناء إرسالها. فالشّبكة التي تنقل بواسطتها البيانات (المشفرّة أو غير المشفرّة) قد تكون مشفرة أو غير مشفرة حتى عبر القنوات أو

---

[134] Tim Mather, Subra Kumaraswamy & Shaed Latif: "**Cloud Security and Privacy: An Entreprise Perspective on Risks and Compliance**", Sebastopol, CA: O'Reilly, 2009, p. 62.

[135] Adrian Chen & 'G Creep: "**Google Engineer Stalked Teens, Spied Chats**'", Gawker, September 14, 2010. (Available on: http://gawker.com/5637234) (Accessed on September 13, 2018, at 11:00 AM).

الشّبكات المشفرة، سيظل مقدمو الخدمة يتلقون بيانات غير مشفرة. وعلى العكس من ذلك، قد لا تكون القنوات المشفرة ضرورية عند إرسال بيانات مشفرة جيّداً حيث إن أي مراقب لن يحصل إلّا على بيانات مشفرة.

البند الثاني: حذف البيانات

هناك درجات مختلفة من "الحذف" في السّحابة كما هو الحال مع أجهزة الكمبيوتر، إذا حذف أحد المستخدمين البيانات فقد تنتقل إلى الـ "trash bin" أو "recycle bin"، ولكنها لم تحذف فعلياً وذلك لفترةٍ من الوقت مثلاً لمدّة 30 يوماً أو حتى إفراغ الـ trash. كذلك، عندما ينتهي العقد مع مقدم الخدمة، لا تحذف بيانات المستخدم على الفور ولكن بعد مدّة زمنية وهذا ما قد يفضله المستخدم إذ يعطى مهلة لاستخراج بياناته. كما قد يساعد استخدام هذه الـ trash bins والحذف المتأخر على جوانب أمنية أي السّلامة والتوافر، فقد يكون حذف البيانات عن غير قصد.

ومع ذلك، حتى في حالات الحذف وإفراغ الـ trashs، لا يتم حذف البيانات في الغالب. ولكن يتم حذف "pointers"[136] التي تحتوي على مواقع لبيانات التعريف المرجعية للأجزاء التي تضم مجموعة البيانات ويتم استبدال البيانات الفعلية بشكل تدريجي مع مرور الوقت ببيانات جديدة سواء من قبل نفس المستخدم أو مستخدم آخر، فيمكننا أن نرى هذا البند مثلاً في شروط "Google Apps (Free) Agreement":

"10.3 (iii): After a commercially reasonable period of time, Google will delete Customer Data by removing pointers to it on Google's active servers and overwriting it over time."[137]

ومن ثم، قد تكون مسألة استعادة البيانات، أو ما هو متبقٍ من البيانات التي تم مسحها أو إزالتها، مشكلة. فالأجزاء المتبقية قد تكون إمّا غير مفهومة أو لا يمكن إعادة تركيبها وفقاً لنوع الخدمة والتصميم خاصةً مع أجهزة الـ VM (Virtual Machines) حيث قد تُكشَف للمستخدمين الذين يتشاركون البنية التحتية الأساسية. لذلك تتطلب السّرية الفعلية استبدال البيانات المحذوفة أكثر من مرّة (أي حفظ بيانات مكانها) فيعتبر المنظمون لحماية البيانات أنه يجب حفظ فوق البيانات الشّخصية في السّحابة عدّة مرّات للحذف الصّحيح[138]، الحلّ الوحيد هو الإزالة المغناطيسية أو تدمير وسائط التخزين المادية. ومع ذلك، قد تكون الكتابة فوق البيانات المشفرة جيّداً غير ضرورية أو حتى تدمير المفاتيح وذلك لعدم تمكن مقدمي

[136] Pointers أي المؤشرات هي في الأساس متغيرات يمكن أن تشير إلى موقع آخر في الذاكرة.

[137] "Google Apps (Free) Agreement"
(Available on: http:www.google.com/apps/intl/en/terms/standard_terms.html) (Accessed on September 19, 2018, at 15:12 PM).

[138] Article 29 Data Protection Working Party, Opinion 05/2012 on Cloud Computing, WP 196, p. 12.

الخدمات والجهات الخارجية الأخرى من الوصول إلى مفاتيح المستخدمين.[139] ومع ذلك، من الصّعب حذف البيانات بشكل انتقائي من الأشرطة الاحتياطية المجمعة. كذلك، قد لا يسجل مزوّد الخدمة بيانات المستخدم على نسخ احتياطية فحذف النسخة الأصلية يؤدي إلى حذف جميع النسخات.
كما وأن حذف البيانات بشكل آمن قد يتطلب الحذف من مواقع ووسائط متعددة، وتوجد مستويات مختلفة للحذف تصل إلى تدمير الأجهزة المادية وهذه الطريقة قد تؤدي إلى وجود مشكلة بالتكلفة المالية على قدر من المشكلة الفنية، إذ إنها مكلفة جداً. علاوة على ذلك، فإن بعض خدمات تخزين SaaS تقدم ميزة عدم تدمير البيانات، والاحتفاظ بجميع إصدارات الملفات مما يتيح للمستخدمين استرداد كل ما هو قديم مثلاً "DropBox"، وبالمثل، إن بعض أنظمة مراكز البيانات تحتفظ تلقائياً بنسخ "محذوفة".[140]

الفقرة الثانية: حالة الخدمة

يجب أن يؤمّن المزوّد للمستخدمين خدمة متوافرة عند الطلب ومرونةً وأماناً خاصةً عند نقل البيانات كما سنرى في هذه الفقرة؛ إذ إن هذه الصّفات تؤثّر أيضاً في إختيار شركة معينة.

النبذة الأولى: التوافرية Availability

مع استمرار نمو الأنظمة السّحابية من حيث الحجم والتعقيد، من المهم ضمان استقرارها وتوافرها وموثوقيتها. ولكن هذه الموثوقية قد تخرق بسهولة إذا لم يتم اتخاذ تدابير مسبقة للتعامل مع الفشل المحتمل في الأنظمة الفرعية للسحابة. وعليه، سجلت Google خسارة في الأرباح وقدرها 20% عندما تسببت في تأخير قدره 500ms في وقت الإستجابة. كذلك Amazon سجلت انخفاضاً في مبيعاتها بنسبة 1% لتأخير قدره 100ms في نتائج البحث.[141] وبالمثل، فإن فشل التبديل الأساسي في شبكة blackberry ترك ملايين العملاء دون المقدرة للوصول إلى شبكة الانترنت لمدة ثلاثة أيام. إن أي خطأ أو خلل يؤثر على الطرفين سواء مزوّدي الخدمة أو العملاء، يوجب على المزوِّدين اعتماد آليات مختلفة لتخفيف الخطأ على مستوى النظام. Fault Tolerance أي استتابة الخطأ هو قضية حيوية في

---

[139] Christine Drake: "Cloud Data Destruction: Is Your Old Data Still Accessible?", August 15, 2012, posted on trend micro.
(Available on: http://cloud.trendmicro.com/cloud-data-destruction) (Accessed on September 13, 2018, at 16:48 PM).

[140] Supra 72, page 797.

[141] Greenberg A., Hamilto J., Maltz D. & and Palel P.: "**The cost of a cloud: Research problems in data center networks**", 2009, ACM SIGCOMM Computer Communication Review 39(1), pages 68-79.

منصات الحوسبة السّحابية والتطبيقات، إنها تمكن النظام من الاستمرار في التشغيل بمستوى منخفض بدلاً من الفشل التام.

يمكن أن تتخذ الأخطاء أشكالاً مختلفة:

أ. عطل الأجهزة سواء العابرة أو المتقطعة أو الدائمة.

ب. أخطاء البرامج وأخطاء التعميم.

ت. أخطاء المشغل.

ث. أخطاء خارجية.

السّحابة مقسمة إلى عدّة طبقات كما رأينا سابقاً، SaaS ،PaaS و IaaS، وأي خلل أو عطل في طبقة من هذه الطبقات يؤثر على الطبقة التي تعلو. مثلاً أي خلل في PaaS قد يؤدي إلى أخطاء في خدمات البرمجيات المقدمة من SaaS.[142]

النبذة الثانية: المرونة في نقل البيانات

إن مصدر قلق المستخدمين هو خطر الاعتماد أو التقيّد المفرط على الخدمة التي يقدمها مزوّد واحد وهذا ما يسمى بالـ "lock-in" أي ارتباط شخص أو شركة بشركة واحدة وعدم تمكنهم من الانتقال بسهولة إلى مزوّدٍ آخر بدون تكاليف كبيرة أو قيود قانونية أو عدم التوافق الفني والتقني بين الشركتين.[143] وللتأكد أكثر من وجهة نظر مزوّدي الخدمة، فإن الـ lock-in في التطبيقات التي تم تطويرها لمنصات سحابة خاصة مثل Microsoft Azure، Amazon EC2، لا يمكن نقلها بسهولة إلى منصات سحابية أخرى ويصبح المزودون عرضة لأي تغييرات من قبل مزوديهم.[144] في الواقع، تنشأ مشكلة الـ "lock-in" عندما تقرر شركة، على سبيل المثال، تغيير مزوّد الخدمة أو ربما دمج الخدمات من مزوّدين مختلفين، وهي غير قادرة على نقل التطبيقات أو البيانات عبر خدمات سحابية مختلفة نظراً لأن خدمات المزوّدين المختلفين لا تتطابق مع بعضها البعض. إن عدم التجانس بين دلالات السّحابة (cloud semantics) وواجهات برمجة التطبيقات السّحابية (Cloud Application on Program Interfaces (APIs

---

[142] Kashif Bilal, Osman Khalid, Saif Ur Rehman Malik, Muhammad Usman Shahid Khan, Samee U. Khan, and Albert Y. Zomaya: "**Fault Tolerance in the cloud**", published in **Encyclopedia of Cloud Computing**, John Wiley & Sons Ltd., United Kingdom, 2018, p. 291-292.

[143] Michael A., Armando F., Anthony DJ, Randy HK, Andrew K, Gunho L, David AP, Ariel R, Ion S & Matei Z: "**A view of Cloud Computing**", 2010, Commun ACM 53(4):5058.

[144] Stiaram D & Manjunath G: "**Moving to the cloud: developing apps in the new world of cloud computing**", 2012, Elsevier, USA.

يخلق عدم توافق فني يؤدي بدوره إلى تحديات قابلية التشغيل المشترك وقابلية نقل البيانات والخدمات وقابليتها للادارة. ولهذه الأسباب من وجهة نظر الشّركات، من المهم الإبقاء على المرونة في تغيير مقدمي الخدمات، لأنه الطريق نحو سوق أكثر تنافسية لمزوّدي الخدمات السّحابية والعملاء.[145]

المبحث الثاني: السّرية في الحوسبة السّحابية

لماذا نتحدث عن السّرية في الحوسبة السّحابية؟ لماذا السّرية أساسية فيها؟ ما الذي يتطلب سريّة؟ هل هي جميع المعلومات والبيانات المحفوظة على السّحابة؟ ماهية هذة المعلومات؟ ما الفرق بين المعلومات والبيانات؟ هل تكون هذه البيانات مزوَّدة إلى الخادم من قبل المستخدم فقط أو هناك أساليب أخرى لجمع البيانات؟ وهل تكون بعلم أو جهل المستخدم؟ كما ويجب التساؤل حول حماية هذه المعلومات.

الفقرة الأولى: المعلومات المتوجبة السّرية

عندما يقوم الأشخاص بتسجيل الدخول إلى الانترنت وزيارة مواقع الويب المرتكزة على الحوسبة السّحابية، يتم جمع قدر كبير من المعلومـات وخاصةً الشّـخصية منها، أو حتى عند إدخال المعلومات على حسابات، من خلال مشاركة المستخدمين النشطة وتقنيات التجميع السّلبي. تقوم مواقع الويب بجمع المعلومات من خلال مشاركة المستخدمين عندما يقومون مثلاً بفتح حسابات عبر الانترنت أو مسك نماذج الاشتراك أو التسجيل للوصول إلى مواقع "members only" . من الطرق الأساسية لجمع البيانات السّلبية هي: استخدام موقع الويب لملفات تعريف الارتباط (cookies) ومجموعة OSP لبيانات "البث"(click stream).

النبذة الأولى: تحديد المعلومات

في السّحابة، يكون الاستعمال إمّا من قبل أشخاص طبيعيين أو من قبل أشخاص معنويين أو من قبل حكومات كما سبق وذكرنا، فتختلف المعلومات المحفوظة على السّحب من فئة إلى أخرى ولكن يجب على كل فئة من هذه الفئات تصنيف البيانات بناءً على حاجتها إلى السّرية أو الحساسية. فلا يوجد أي جدوى من حفظ جميع البيانات بالطريقة ذاتها لأن بعضها يحتاج إلى أمان أكثر من غيرها. فتأمين كل

---

[145] Justice Opara-Martins, Reza Sahandi and Feng Tian: "**Crtical analysis of vendorlock-in and its impact on cloud computing migration: a business perspective**", Journal of Cloud Computing: Advances, systems and applications (2016)5:4, DOI 10.186/s 1377-016-0054-z.

البيانات بمستوى أمان منخفض يمكّن الوصول إلى البيانات الحساسة بسهولة، وتأمين كل البيانات بمستوى أمان مرتفع يعد مكلفاً للغاية ويقيد الوصول إلى البيانات غير السّرية وغير النقدية. فالتصنيف يستخدم لتحديد مقدار الجهد والمال والموارد التي يجب تخصيصها لحماية البيانات وتقييد الوصول إليها. يتم استخدام التصنيف لتوفير آليات أمان لتخزين البيانات ومعالجتها ونقلها أو إزالتها وتدميرها، ويمكننا ذكر بعض فوائد استخدام نظام تصنيف البيانات:

- يدل على التزام المنظمة أو المؤسسة بحماية الموارد القيمة
- يساعد في تحديد البيانات الأكثر أهمية للمؤسسة
- يمنح المصداقية لاختيار آليات الحماية
- يساهم في الامتثال التنظيمي أو القيود القانونية[146]

وبالرغم من أن الكثير من البيانات قد تكون حسّاسة وبحاجة إلى سرية إلّا أن القوانين والأنظمة لم تهتم سوى بالبيانات الشّخصية فغدت الحالة أنه عند التكلم عن الحوسبة السّحابية نتكلم تلقائياً عن حماية البيانات ذات الطابع الشّخصي، فمثلاً القانون اللّبناني رقم 2018/81 يتعلق بالمعلومات الالكترونية والبيانات ذات الطابع الشّخصي، كما والتنظيم العام لحماية البيانات (The General Data Protection Directive GDPD) الصّادر عن المفوضية الأوروبية مرتبط بالبيانات ذات الطابع الشّخصي وغيرها من القوانين والأنظمة، إذ لم تعطِ كامل البيانات الأهمية التي أعطيت للبيانات ذات الطابع الشّخصي، وتستند هذه القوانين إلى مبادئ موحدة متناسقة لاسيما المبادئ التوجيهية لمنظمة التعاون والتنمية OECD لعام 1980 [147]، فما هي البيانات ذات الطابع الشّخصي؟

جاء تعريف البيانات الشّخصية وفق مبادئ OECD لعام 1980 على الشّكل التالي:

"Means any information relating to an identified or identifiable individual (data subject)".

تعني أنّها أي معلومة تتعلق بفرد محدد أو قابل للتحديد (موضوع البيانات). وقانون 2018/81 عرّفها بأنها جميع أنواع المعلومات المتعلقة بشخص طبيعي التي تمكن من التعريف به، على نحو مباشر أو غير مباشر، بما في ذلك عن طريق مقارنة المعلومات المتعددة المصادر أو التقاطع فيما بينها. أمّا الـ GDPR عرّفها:

---

[146] Office of the Minister of State for Administrative Reform: "**Lebanese National Cyber Security Policy Guidelines**", November 27, 2015, page 15-16.

[147] المبادئ التوجيهية التي تحكم حماية خصوصية وتدفق البيانات الشّخصية عبر الحدود (Guidelines governing the protection of privacy and transborder flows of personal data) (Available on: http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm) (Accessed on August 30, 2018 at 12:12 PM).

“Any information relating to an identified or indentifiable natural person (‘data subject’), an identifiable natural person is one who can be identified directly or indirecdtly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, cultural or social identity of that natural person.”[148]

أي أنها المعلومات التي تتعلق بشخص طبيعي محدد أو قابل للتحديد ("موضوع البيانات"). الشّخص الطبيعي المحدد هو الشّخص الذي يمكن تحديده إمّا بشكل مباشر أو غير مباشر، بشكل خاص بالرجوع إلى معرّف مثل الإسم، رقم التعريف، بيانات الموقع، معرّف عبر الانترنت أو إلى واحد أو أكثر من العوامل المحددة للفيزيائية، الفيزيولوجية، الهوية الجينية أو العقلية أو الاقتصادية أو الثقافية أو الإجتماعية لهذا الشّخص.

وهذا التعريف الأخير مهم إذ إنه يلائم التطور في التكنولوجيا وطريقة جمع البيانات عن الأشخاص من قبل المنظمات. البيانات الشّخصية الحساسة هي تلك التي تكشف عن الأصل العرقي، الآراء السّياسية، المعتقدات الدينية أو الفلسفية أو العضوية النقابية، أو البيانات المتعلقة بالصّحة أو الحياة الجنسية والجرائم والإدانات الجنائية.[149] ونرى بالتالي أن جميع البيانات الشّخصية تخضع للـ GDPR والبيانات الشّخصية الحساسة تخضع لقواعد أكثر صرامة. أمّا في القانون اللّبناني ليس هناك من تفريق بين البيانات الشّخصية وحتى ليس هناك تفصيل لهذه البيانات وسواء كانت محذوفة أومشفرّة أو تحت اسم مستعار ولكن يمكن استخدامها لإعادة تحديد هوية شخص ما، فتعتبر بالتالي بيانات شخصية وتخضع للقوانين.

---

[148] Article 4 of the ‘Regulation (EU) 2016/679 of the European Parliament and of the council of 27 April 2016’ on the protection of natural persons with regard to the processing of personal Data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[149] Article 9.(1) of the GDPR: “Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifiying a natural person, data concerning health or data concerning a natural persons sex life or sexual orientation shall be prohibited.”

أمّا البيانات التي تم الكشف عنها بطريقة تجعل الشّخص غير قابل لتعريف لا تعد بيانات شخصية، فلكي تكون مجهولة المصدر يجب أن يكون إخفاء الهوية أمراً لا رجوعاً فيه.[150]

النبذة الثانية: أساليب مختلفة لتجميع المعلومات

كما سبق وذكرنا أننا نشهد يومياً تطوراً في التكنولوجيا، وهناك أساليب جديدة في كل إطار في العالم السّيبراني، من ضمنها طرق تجميع المعلومات، إذ إنها متنوّعة وعديدة. فقد لا يعرف المستخدم العادي أن ما ينقر عليه يعطي الطرف المقابل الحق في الحصول وحفظ معلومات شخصية عنه.

البند الأول: استعمال المواقع للـ cookies

"ملف تعريف الارتباط" أو "cookie"[151] هو عبارة عن ملف نصي صغير يرسله موقع ويب ليتم تخزينه على محركات الأقراص الثابتة (hard drive) لزوار الموقع.

تحتوي الـ cookies على معلومات حول مواضيع مختلفة، بعضها متعلق بعدد الزيارات التي يقوم بها المستخدم إلى موقع ويب معين، بينما يقوم الآخرون بمتابعة كلمات المرور والتفضيلات الخاصة بالمستخدم. قد لا يعلم المستخدم أن معظم المواقع ترسل cookies لأن معظم المتصفحات (browsers) لديها "no cookie warning"، بالرغم من أن معظم المتصفحات لديها القدرة على إعلام المستخدم أنه يتم إرسال "cookie" وآلية رفضها من قبل المستخدم. ومع ذلك، النظام الإفتراضي no cookies warning يؤدي إلى عدم معرفة المستخدم بكمية ملفات الـcookies التي يتم إرسالها إلى محركه أو مكان إرسالها.

قد تخترق أو تهدد الـ"cookies" خصوصية المستخدم بطريقتين أساسيتين:

أولاً، يتم تخزين الـcookie على القرص الثابت للمستخدم ويمكن الوصول إليها بوقت لاحق. بمجرد الوصول، ستعرض قائمة مفصلة بكل موقع ويب تمت زيارته بواسطة هذا الكمبيوتر خلال نطاق زمني محدد. علاوة على ذلك، قد يكشف الملف عن معلومات شخصية عن المستخدم، مثل كلمة المرور، عنوان البريد الإلكتروني أو أية معلومات أخرى تم إدخالها عند تواجده على هذا الموقع. مثلما حدث عندما إكتشف مسؤولون حكوميون أن John Deutch، الرئيس السّابق لوكالة المخابرات المركزية CIA، إستخدم حاسوبه المنزلي لكتابة مذكرات في غاية السّرية. وبعد بحثٍ لاكتشاف مدى الأضرار التي لحقت

---

[150] https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data-en. (Accessed on August 29, 2018 at 22:41 PM).

[151] تم اقتباس اسم "cookie" من مصطلح "magic cookie" والذي يشير إلى حزمة قصيرة من البيانات التي يتم تبادلها بين برنامجين متصلين.

بالأمن القومي، اكتشفت الـ FBI على حاسوبه، cookies تظهر زيارته لمواقع ترفيه للكبار والتي وصفتها وكالة المخابرات المركزية بأنها "عالية المخاطر".[152]

ثانياً، إن الطريقة التي قد تؤثر بها الـ cookies على الخصوصية هي أن خوادم مواقع الويب التي ترسل هذه الملفات تتلقى أيضاً المعلومات المخزنة في الـ cookies عندما يقوم المستخدم بإعادة زيارة الموقع نفسه. باستخدام الـcookies، تمتلك مواقع الويب حالياً القدرة على تتبع الموقع الذي جاء منه المستخدم والروابط التي نقر عليها أثناء وجوده في الموقع، وأية عملية شراء تم إجراؤها، وأية معلومات شخصية تم إدخالها. كما أن العديد من الـ cookies قادرة على تحديد عنوان بروتوكول الانترنت (IP address) للمستخدم، مما يمنحها القدرة على تحديد الموقع الدقيق للحاسوب المستخدم للوصول إلى موقع الويب.[153] وبمجرد أن يجمع موقع الويب هذه المعلومات قد يستخدمها بطرق تنتهك خصوصية موضوع البيانات. على سبيل المثال، يمكن للمرأة أن تختار شراء اختبار للحمل من متجر على الانترنت معتقدةً أن هذه الطريقة مؤكدة للإبقاء على عدم الكشف عن هويتها في مواجهة مثل هذه المسألة الشّخصية، ومع ذلك قد يختار موقع الويب تفكيك المعلومات المتعلقة بشرائها وعنوان بريدها الإلكتروني إلى المؤسسات المؤيدة للحياة والتي يمكن أن تغمرها بالرسائل عبر البريد الالكتروني.[154]

كذلك، من خلال نشر "اعلانات الراية" (banner ads) [155] يمكن لشركات التسويق المباشر تجسيد ممارسات جمع المعلومات على الانترنت. كانت إحدى هذه الشّركات "Double Click" موضوع تقاضي وقلق عام هائل في أوائل القرن العشرين[156]، Double Click مثل العديد من شركات التسويق المباشر

---

[152] Nile Latham: "**Too Big for his Breaches: CIA Ex-Chief Free as Scientist is Jailed for Same Offense**", N.Y. Post, March 8, 2000.

[153] Domingo R. Tan: "**Comment, Personal Privacy in the Information Age: Comparison of Internet Data Protection Regulations in the United States and the European Union**", 21 LOY.L.A.INT'L & COMP. L.J.661, 666 (1999).

[154] Rachel K. Zimmerman: "**The Way the "COOKIES" Crumble: Internet Privacy and Data Protection in the Twenty-First Century**", Legislation and Public Policy, vol 4:439, unknown publisher and publishing year. (Available on: http://www.nyujlpp.org/wp-content/uploads/2012/11/Rachel-K.-Zimmerman-The-Way-the-Cookies-Crumble-Internet-Privacy-and-Data-Protection-in-the-Twenty-First-Century.pdf) (Accessed on September 19, 2018 at 20:31 PM).

[155] Banner ads هي وسيلة تسويق إلكتروني على الانترنت عبر خوادم للإعلان.

[156] In re DoubleClick Inc. Privacy Litigation, No. 1352, 2000 U.S. Dist. LEXIS 11148, (Available on: https://law.justia.com/cases/federal/district-courts/FSupp2/154/497/2429654) (Accessed on September 23, 2018, at 09:47 AM).

على الانترنت، تنشر إعلانــات banner على مواقع الويــب الخاصة بشركات أخرى. إعلانات الـ banner تخدم غرضاً مزدوجاً: تعلن منتجات عملاء DoubleClick أثناء جمع المعلومات من خلال استعمال الـcookies، عن كل زائر للموقع الذي يتم عرض إعلان الـ banner عليه.
على الرغم من أن معظم مواقع الويب لديها القدرة المحدودة فقط لقراءة ملفات الـ cookies من القرص الصّلب للمستخدم الذي أرسله الموقع نفسه في زيارة سابقة، فإن إعلانات الـ banners لديها قدرة أكبر على مراقبة سلوك المستخدمين على الانترنت. يمكن نشر إعلانات الـ banner على مئات المواقع المختلفة ويمكنها إرسال ملفات الـ cookies المرتبطة بها بالإضافة إلى تلك الخاصة بموقع الويب نفسـه. قد تحتوي الـ banner ad cookies على نفس المعلومات عن المستخدم المضمنة في ملفات تعريف الارتباط الخاصة بموقع ويب، وتتمتع بقدرة إضافية على قراءة ملفات تعريف الارتباط التي ترسلها إعلانات الـbanner الأخرى الموجودة في مواقع مختلفة طالما أن نفس شركة التسويق تملك الإعلانين. وبهذه الطريقة، تستخدم شركات التسويق مثل DoubleClick الـ cookies لجمع كميات هائلة من المعلومات الشّخصية عن المستخدمين غير المرتابين.[157]

البند الثاني: مجموعة OSP [158] لبيانات البث

كما تقوم مواقع الويب وشركات إعلانات الـbanners بجمع المعلومات من خلال استخدام الـcookies، قد تقوم الـ OSPs بمراقبة وتسجيل معلومات المشتركين الخاصة بهم من خلال استخدام بيانات click stream[159] لأن المستخدمين، عند اتصالهم بالانترنت باستخدام OSP يمكّنون هذه الأخيرة تسجيل معلومات مثل المواقع التي يزورونها والروابط التي ينقرون عليها من كل موقع.
تمتلك OSPs أيضاً القدرة على غزو خصوصية مشتركيها من خلال السّماح بالاتصال بالمعلومات الشّخصية التي يحتاجونها من المستخدمين لديهم ويمكننا ذكر قضية McVeigh v. Cohen حيث تم تسريح ضابط من البحرية الأمريكية بعد أن أعطت الـ OSP (America Online AOL) معلومات خاصة به لرؤسائه سمحت لهم ربط اسمه مع بريده الإلكتروني بعد أن اعترضت البحرية رسالة مكتوبة من حساب البريد الالكتروني الخاص به فيما يتعلق بالمثلية الجنسية. بينما صحيح أن الضابط أعطى

---

[157] Supra 154

[158] Open Settlement Protocol : OSP : بروتوكول بين العميل والخادم يقوم بإدارة التحكم في الوصول والمحاسبة وبيانات الإستخدام والتوجيه بين النطاقات لتسهيل مزودي خدمات الانترنت لدعم المهاتفة عبر بروتوكول الانترنت (IP Telephony)

[159] Click stream يعد عبارة عن سجل لنشاط المستخدم على الانترنت بما في ذلك كل موقع ويب وكل صفحة من صفحات كل موقع ويب يقوم المستخدم بزيارتها، أو المدة التي كان فيها المستخدم في صفحة أو موقع أو ترتيب الصّفحات التي تمت زيارتها أو أية مجموعات أخبار.

AOL اسماً له عندما قام بالتسجيل لدى الشّركة للحصول على عنوان البريد الالكتروني، صحيح أيضاً أنه من المتوقع أن تكون قادرة على إرسال واستقبال رسائل البريد الالكتروني غير الضارة مع درجة معينة من عدم الكشف عن هويته ولكن أضعف AOL هذا التوقع عندما عرض المعلومات الشّخصية على رؤسائه.[160]

الفقرة الثانية: عوائق السّرية

السّريّة التي يطالب بها المستخدم ويبحث عنها في الشّركات التي يتعاقد معها قد تخترق سواء من قبل المزوّد بحدّ ذاته، أو من قبل أطراف ثالثين إن بقيامهم بعمل مخالف للقوانين أو بموجب قوانين داخلية أم أجنبية تسمح بالوصول إلى البيانات.

النبذة الأولى: حق المزوّد بالحصول على المعلومات

تتأثر فعالية تدابير منع الأشخاص غير المستخدمين من الوصول إلى بيانات المستخدم الشّخصية المخزنة وغير المشفرة، بكون البيانات "بيانات شخصية" فيما أو لا. إن العامل الأساسي هو فعالية نظام التحكم في الوصول الذي لا يسمح عادةً إلّا للمستخدمين الموثوقين والمصرح لهم بالوصول إلى حساب سحابة معين. عن طريق تسجيل الدخول إلى حساب، يمكن للمستخدم الوصول إلى مجموعة كاملة من أي بيانات شخصية مخزنة وتشغيلها. مع ذلك، هذا لا يعني أن الآخرين يمكنهم الوصول إلى البيانات. من شأن المزيد من تدابير مراقبة الدخول الفعالة والمقيدة أن تزيد من احتمال استبعاد الآخرين من إعادة تحديد الهوية وبالتالي لن تشكل البيانات المخزنة "بيانات شخصية". كذلك قوة كلمات مرور المستخدمين قد تؤثر على فعالية تدابير التحكم في الوصول. فيؤثر عنصر تحكم المستخدم بدلاً من المزوّد في حالة اختيار كلمة مرور قوية، في ما إذا كانت المعلومات التي يحتفظ بها هي شخصية أو لا.[161]

---

[160] 983 F. Supp. 215 (1998): **Timothy R. McVEIGH, Plaintiff, v. William S. COHEN, et al., Defendants**, No. CIV. A. 98-116. United States District Court, District Columbia. January 26, 1998.
(Available on: https://law.justia.com/cases/federal/district-courts/FSupp/983/215/1989052/) (Accessed on September 25, 2018 at 10:03 AM).

[161] W. Kuan Hon, Christopher Millard & Ian Walden: "**The Problem of “Personal Data” in Cloud Computing- What Information is Regulated? (The Cloud of Unknowing, Part 1)**", Queen Mary University of London, School of Law, Legal Studies Research Paper No. 75/2011, 10 March 2011, p. 33.

من العوامل المهمة الأخرى، وجود "backdoors" تسمح للمزودين بتسجيل الدخول إلى حسابات المستخدمين أو الوصول إلى بيانات المستخدمين المعاد جمعها. من مزايا الحوسبة السّحابية أن مزودي الخدمة عادةً يحتفظون ويقومون بالتحديث التلقائي لبرنامج تسجيل الدخول وبرنامج (SaaS) للتطبيقات، في حين أنه ملائم للمستخدمين، لكنه يعني أيضاً أنه يمكن للمزودين بدون علم المستخدم انشاء واستخدام الـ"backdoors"، أو حتى إنشاء backdoors بناء على طلب من السّلطات القانونية أو الأمنية أو غيرها.[162] في حين أن المعدات التي تحتوي على بيانات شخصية مجزأة قد يتم ضبطها، وقد يتم الوصول غير المرغوب به إلى البيانات من خلال قدرة المزوّد على الوصول أو السّماح لأطراف ثالثة بالوصول والحصول على المعلومات أينما كانت الخوادم موجودة حتى لو في دولٍ أخرى. مثلاً يتمتع المهندسون الموثوقون بموقع Google بـ "الوصول غير المقيّد إلى حسابات المستخدمين للخدمات التي يشرفون عليها". في عام 2010 تم طرد أحد هؤلاء المهندسين بسبب الدخول إلى حسابات Google الخاصة بالقاصرين دون موافقة، بما في ذلك سجلات المكالمات وتفاصيل الاتصال من خدمة هاتف الانترنت وقوائم جهات اتصال المراسلة الفورية.[163] هل هذه الحالة تعتبر مجرد مخالفة نظامية؟ مخالفة لأنظمة الشّركة؟ أم أيضاً مخالفة للقوانين؟ ألا تعتبر ولوجاً غير مصرّح به أي ولوج غير مشروع لمعلومات؟ إذ إن ولوجه إلى النظام مصرّح به في إطار عمله ولكن تعديه لهذا التصريح يؤدي إلى دخوله للنظام بطريقة غير مشروعة تعاقب عليها القوانين من ضمنها القانون اللّبناني 2018/81 في مادته 110.

يمكن ملاحظة أن امتلاك الحق القانوني والقدرة الفنية للوصول إلى البيانات لا يعني الوصول الفعلي إليها. فلا يعرف المزوّد إلّا عند وصوله إلى المعلومات أنها شخصية. قد يكون من المعتقد أن المزوّد الذي يقوم بتقييد الوصول إلى عدد قليل جداً من الموظفين، لا يسمح به إلّا بظروف خاضعة للرقابة الصّارمة، ويتخذ الاجراءات التقنية والتنظيمية الأخرى مثل فحص سجلات الوصول بشكل منتظم، يتعرضون لمسؤولية أقل من مقدم الخدمة الذي يسمح لجميع الموظفين بالوصول إلى جميع بيانات المستخدمين في أي وقت ولأي غرض يرغب فيها أي موظف.[164]

بالإضافة إلى إمكانية ولوج المزوّد إلى البيانات أو تمكين غيره من ذلك، يمكنه الاستفادة منها مادياً، فقد غدت للبيانات الشّخصية قيمة اقتصادية بحيث انتشرت مؤخراً ظاهرة "تجارة البيانات

---

[162] David Drummond: "**Greater Transparency Around Government Requests**", Google Public Policy Blog, April 20, 2010.

(Available on: https://googlepublicpolicy.blogspot.com/2010/04/greater-transparency-around-government.html) (Accessed on September 13, 2018 at 11:12 AM).

[163] Supra 135.

[164] Supra 161, p. 34 .

الشّخصية"[165] وذلك باستغلال بيانات المستخدم وجمعها من معلومات تتعلق باسمه ورقم هاتفه وقائمة بأرقامه وأصدقائه والـ IP address ومعلومات تحديد الموقع الجغرافي GPS، وسجلات البرامج المعلوماتية وغيرها، وذلك للاستفادة منها تجارياً ومادياً، فتبيعها لشركات تسويقية أو تستخدمها بطريقة لتحسين استخدام الخدمة من قبل المستخدم.

مثلاً إن شركة Google شفافة في ما خص هذا الموضوع، فهي تعلن بطريقة واضحة أنها لا تبيع البيانات الشّخصية ولكن بما أن جزءاً كبيراً من أعمالها يعتمد على عرض الإعلانات سواء على خدمات Google أو على مواقع الويب وتطبيقات الجوال التي تشترك مع هذه الشّركة فتستخدم البيانات لغرض هذه الإعلانات ولكن لا تبيع البيانات الشّخصية مثل الاسم وعنوان البريد الالكتروني ومعلومات الدفع، وهذا ما يجعل خدمتها مجانية كما وأنها تضمن إبقاء نقل المعلومات بين الأجهزة آمناً كما وتقول أنها لا تعطي السّلطات أي حق بالدخول إلى البيانات كذلك ليس لديها أي backdoor لأية معلومة.[166] لكن ماهي درجة مصداقية وشفافية الشّركة عند التطبيق؟

كما وأن شركة Facebook لا تبيع البيانات الشّخصية للمستخدم إلّا أنها تبيع إمكانية الوصول إلى حسابك خاصة الـ NewsFeed الخاص بك، وتستخدم البيانات المجمعة عن المستخدم بغرض بث الإعلانات التي تتوافق مع ذوق المستخدم.[167] فهي تقدم خدمة مجانية مقابل الاستفادة مادياً من البيانات التي تجمعها عن المستخدمين ولكن FaceBook لم تمنع مشاركة بيانات شخصية عن المستخدم عندما يستخدم حساب فايسبوك الخاص به لتسجيل الدخول في تطبيقات أخرى، بالرغم من أنها اختزلت بعض البيانات ومنعت مشاركتها ولكن لم تمنع المشاركة بالبيانات كليًّا، وهذه الشّركات التي تعود لها التطبيقات قد تقوم ببيع البيانات المشاركة معها. وعند الخروج من تلك التطبيقات تبقى المعلومات لديها ولكن ليس بإمكانهم الحصول على معلومات إضافية.[168]

---

[165] QUEMENER (Myriam) & PINTE (Jean-Paul) : "**L'économie à l'ère numérique- in : Cyber-Sécurité des acteurs économiques- risques, réponses stratégiques et juridiques**", 2013, Lavoisier, Paris, p. 165.

[166] Tod Haselton: "**How to find out what Google knows about you and limit the data it collects**", December 6, 2017, published on cnbc.com. (Available on: https://www.cnbc.com/2017/11/20/what-does-google-know-about-me.html) (Accessed on September 15, 2018 at 15:23 PM).

[167] Facebook Data Policy available on: https://m.facebook.com/about/privacy/ (Accessed on September 15, 2018 at 16:00 PM).

[168] Kristen Korosec: "**This is the personal data that Facebook collects- and sometimes sells**", March 21, 2018, published on fortune.com. (Available on: http://fortune.com/2018/03/21/facebook-personal-data-cambridge-analytica/) (Accessed on September 15, 2018 at 13:25 PM).

وهناك شركات تبيع بيانات مستخدميها وعملائها وموظفيها إلى شركات تسويقية، يمكننا ذكر حالة المواطن اللّبناني الذي يصله يومياً الكثير من النصوص الهاتفية SMS وe-mails من شركات ومؤسسات وأشخاص بدون إعطائهم الإذن للقيام بهذا الأمر. فيتم عرض بيانات اللّبنانيين على يد شركتي الهاتف المحمول ALFA وMTC touch، والشّركات الإعلانية التي تقدم خدمة إرسال رسائل نصية أو بريد إلكتروني اعتماداً على طلب العميل. تعترف شركتا ALFA وmtc ببيع بيانات المشتركين إلى الشّركات أو الأفراد الذين يرغبون في إرسال رسائل نصيّة إلى مجموعة مستهدفة على النحو المحدد حسب الجنس والعمر والمهنة وفقاً لمواقع الويب على كل من ALFA [169] وmtc [170] وهي البيانات التي تحصل عليها الشّركات عند شراء الناس خطوطاً مسبقة الدفع أو الذين يحولون خطوطهم postpaid. إلّا أنهم يعطون أرقام الهواتف على أساس طلب الشّاري فيكون مستهدفاً فئة معينة من الأشخاص مثلاً الذين تتراوح أعمارهم ما بين 18 و25 عاماً، محل الإقامة... فترسل الشّركة لهذه الفئة الرسائل وتعطي الشّركة الطالبة لائحة بالأرقام ولكن مشفرة وبعدها يمكن للشركة طلب بعض الأرقام كاملة لكي تسأل صاحب الرقم عمّا إذا كان يعود إلى الفئة المستهدفة وبالتالي التأكد من مصداقية شركة Alfa أو mtc.[171]

بالتالي، على هاتين الشّركتين أن تبقيا شفّافتين بتعاملهما مع مستخدمي خدماتهما وإعلامهم عن إمكانية إعطاء معلومات لشركات تسويق مع التأكيد على عدم الإفصاح عن هويتهم إذ تبقى المعلومات غير معرّفة وبالتالي تحافظان على السّريّة في حفظهما للبيانات. إلّا أنه في التطبيق العملي، يمكن لهاتين الشّركتين استعمال البيانات كيفما تشاءان ولن تعاقبا إذ إنهما محتكرتين للسّوق اللّبناني ولا يمكن للإنسان اليوم العيش دون هاتف خليوي.

النبذة الثانية: الاختراق

كل ما هو غير قانوني يكون مخالفاً لأحكام القوانين أو يكون مجرّماً في هذه القوانين، والولوج غير المشروع إلى أنظمة والحصول على بيانات هو عمل جرمي نصّت عليه قوانين داخلية وخارجية؛ تتعدد أساليب هذا الولوج أو الإختراق بسبب التطور واستحداث الأنظمة؛ فلكل نظام ثغرات يمكن للمحترفين إستخدامها للإختراق.

---

[169] Alfa Website (n.d). **Description of service**. Alfa Media. Retrieved from: https://www.alfa.com.lb/en/business/alfa-media. (Accessed on September 10, 2018 at 12:05 PM).

[170] Touch Website.(n.d). **SMS Advertising**. Mobile Media. Retrieved from: https://www.touch.com.lb/autoforms/portal/touch/business/sms-advertising-mobile-media. (Accessed on September 10, 2018 at 13:29 PM).

[171] Elham Barjas & Hussein Mehdy: "**Building Trust: Toward a Legal Framework that Protects Personal Data in Lebanon**", SMEX, Beirut, 2017, p. 14.

البند الأول: Hackers

لقد سمع الجميع بمصطلح Hackers ونربطه تلقائياً باختراق غير مصرح له وبطريقة غير قانونية. هناك عدّة تعاريف لهذا المصطلح على الويب. عند دمج كل هذه التعاريف نحصل على عشاق الكمبيوتر الذين يتمتعون بتعلم لغات البرمجة وأنظمة الكمبيوتر، وغالباً ما يمكن اعتبارهم خبراء في هذا الموضوع، والذين يتمتعون في فن وعلم صناعة أجهزة الكمبيوتر والبرمجيات أكثر بكثير من المصممين الأصليين المقصودين. فالمستللين (hackers) قاموا ببناء الانترنت، وبناء شبكة الانترنت العالمية...[172]
مصطلح hacker واسع جداً وقد يشمل في طيّاته مصطلح cracker أي من يقوم بكسر الشّيفرة؛ وقد يقوم الـ hackers أو بعضٌ منهم بكسر واختراق هذه الأشياء والدخول إليها بدون تصريح للإيذاء أو للسرقة.

بالتالي، هناك فئتان من القراصنة، white hat hacker الذين يبنون ويستخدمون الانترنت للتطوير وblack hat hacker الذين يدمرون كل ما يبنى ويهددون السّلامة والأمان والسّرية في الانترنت.
يخرق الـ crackers القوانين لعدد من الأسباب، وذلك في ترتيب من الأقل ضرراً للأكثر ضرراً:

- يعرفون كيفية القيام بالاختراق
- يحبون التحدي لكسر شيء آمن للغاية
- يحصلون على زحمة من القيام بالأنشطة غير القانونية ويأملون ألا يتم القبض عليهم
- يسعون للشهرة والدعاية
- يريدون الانتقام
- يتقاضون مقابل الاختراق (بالرغم من أن معظمهم يتحمسون للاختراق مجاناً)[173]

صنّف مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاملة المجرمين اعتباراً من عام 2010 خمس جرائم مثل الجريمة السّيبرانية:

1. الوصول غير المصرح به،
2. تلف بيانات أو برامج الكمبيوتر،
3. التخريب لإعاقة عمل الكمبيوتر، النظام أو الشّبكة،

---

172 Raymond E.: "**What is a Hacker?**", 2010, published on catb.org. (Available on: http://www.catb.org/nest/faqs/hacker−howto.html) (Accessed on September 12, 2018 at 10:25 AM).

173 Nataliya B. Sukhai: "**Hacking and Cybercrime**", (Available on: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.470.3895&rep=rep1&type=pdf) (Accessed on September 12, 2018 at 11:00 AM)

4. الاعتراض غير المصرح به للبيانات،
5. التجسس على الكمبيوتر.[174]

وبالتالي الحصول على البيانات والوصول غير المصرح به يعتبر جريمةً، وللمتسللين الكثير من الطرق والأساليب للدخول إلى الجهاز والحصول على البيانات، سواء بإرسال ملفٍ يخوّله الحصول على تصريح بالدخول إلى الجهاز الخاص بالشّخص الذي يفتحه... أو بسبب ضعف كلمات المرور، أو بسبب ضعف الحماية الموفرة من قبل مزوّد الخدمة... وبالتالي أصبحت المعلومات المتعلقة بالشّخص بحوزة شخص آخر ولكن هل هي فقط بحوزته؟ أو يمكنه نشرها أو بيعها؟

بالطبع، لا يتم الاختراق بهدف الحصول على المعلومات وعدم التصرف بها إلّا إذا كان السّبب شخصياً بحتاً بين المقرصن والضحية. عدا هذه الحالة، البيانات ستنتشر أو تعرض للبيع أو تعطى لطرف ثالث أو تتعرض الضحية للابتزاز. أين تباع هذه البيانات؟

بما أن عمل الحصول على البيانات بطريقة الـ hacking هو عمل جرمي، بالتالي كل تبعاته هي أعمال جرمية خاصة بيعها، فيعاقب الـ hacker على جريمتين. ولو كان البيع قانونياً، لتم بطريقة علنية وليس على الـ Dark Web أو Dark Net وهما متفرعان من الـ Deep Web حيث توجد مواقع تبيع المخدرات، وبرامج القرصنة والبيانات وغيرها من الأمور غير الشّرعية... فماهي قيمة الفرد في هذه المواقع أي قيمة معلوماته الشّخصية؟

فقام Fractl بالدخول إلى الـ Dark Web لإعداد تقريره، إذ هناك طريقة محددة للدخول إليها عبر TOR وبإخفاء هوية الشّـــــخص إذ هذه المواقع مراقبة من قبل جهات أمنية، وكانت المفاجأة أن الدخول إلى الـ Facebook يمكن أن يباع فقط بـ 5.20$ وذلك لأنه يسمح للمجرم بالحصول على معلومات شخصية تسمح له بالوصول إلى معلومات أكثر للشخص.

ويمكن الحصول على هوية الانترنت كاملة لشخص ما، بما في ذلك أرقام التعريف الشّخصية والحسابات المالية المخترقة، مقابل 1200$ فقط ذلك لأن الكثير من المعلومات الشّخصية قد تكون متاحة بالفعل للمقرصنين بسبب الخروقات المتكررة للبيانات التي قد قاموا بها.[175]

---

[174] **Tenth United Nations Congress On Prevention of Crime and Treatment of Offenders Opens in Vienna**, Press Release SOC/CP/216, April 10, 2000.

(Available on: https://www.un.org/press/en/2000/20000410.soccp216.doc.html) (Accessed on August 15, 2018 at 19:00 PM).

[175] Maria LaMagna: "**The Sad Truth about how much your facebook data is worth on the dark web**", June 6, 2018, published on marketwatch.com.

(Available on: https://www.marketwatch.com/story/spooked-by-the-facebook-privacy-violations-this-is-how-much-your-personal-data-is-worth-on-the-dark-web-2018-03-20) (Accessed on September 15, 2018 at 22:14 PM).

كذلك هناك معلومات مصرفية تباع على هذه المواقع، وخاصة الـ credit cards بتزايد مستمر يفوق الـ 100% في السّنة.[176]

وفي هذا المجال لا يسعنا إلّا ذكر قضية خليل الصّحناوي التي شغلت ولا تزال تشغل الرأي العام والقضاء والجهات الأمنية اللّبنانية، بالرغم من أنها لا تتعلق بالسّحابة إذ إن الدولة اللّبنانية وجهاتها الأمنية لا تعتمد على السّحابة ولكن تحتفظ بالمعلومات على خوادم خاصة بها، ولكن يجب ذكر هذه القضية عن القرصنة إذ إنها طالت بيانات عشرة آلاف من اللّبنانيين. اخترقت خصوصياتهم وتعرّض البعض للابتزاز، فدخل خليل الصّحناوي إلى داتا أوجيرو وأجهزة أمنية وأتاح القراصنة له التلاعب بمضمون هذه البيانات والتنصت على اتصالات الهاتف الثابت، والحصول على البريد الالكتروني وكلمة المرور لمدير عام جهاز أمني والضابط المسؤول عن الشؤون التقنية في الجهاز، فضلاً عن اختراق البريد السّري للمديرية الأمنية وقرصنة مواقع وزارتي الداخلية والاقتصاد وقوى الأمن الداخلي والأمن العام وعدد من المصارف دون ترك أثر خلفه. فوجدت بيانات حسّاسة للغاية على أجهزته المختلفة وهي مشفرة إذ يصعب فك هذا التشفير وقال إنه يحتفظ بها على سبيل الحشرية ولم يعترف من هي الجهة التي يعمل لها.[177]

ولكن يطرح السّؤال حول سبب ضعف أنظمة الحماية في أجهزة الدولة الأمنية التي لا تعتمد السّحابة بل لديها خوادمها الخاصة التي يجب أن تكون أكثر أماناً، كذلك في بعض المصارف التي تتبع السّرية المصرفية ويجب أن تكون حماية البيانات لديها فعالة جداً، فما حال الدولة اللّبنانية إذا انتقلت إلى السّحابة؟ هل ستتمكن من تأمين الحماية اللّازمة لبيانات ومعلومات مواطنيها؟

البند الثاني: دور القانون الأميركي

"USA PATRIOT Act"[178] قانون لمكافحة الإرهاب، اعتمدته الولايات المتحدة عَقبَ هجمات 11 أيلول 2001 [179]، تم إصداره كقانون طوارئ في ظل الأوضاع الأمنية المضطربة في البلد، وتم

---

[176] Cash Card: "**Report: Bank Data for Sale on the Dark Web Rise By 135% Every Year**", August 3, 2018, published on deeptoweb.com.
(Available on: https://www.deeptoweb.com/2018/08/03/report-bank-data-for-sale-on-the-dark-web-rises-by-135-every-year/) (Accessed on September 16, 2018 at 08:16 AM).

[177] جريدة الأخبار: صحناوي تجسس على كل لبنان، 14 أيلول 2018، https://al-akhbar.com/Politics/257921.

[178] USA PATRIOT Act :Uniting and Strengthering Americ a by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act.

[179] أحداث 11 أيلول 2001 مجموعة هجمات شهدتها الولايات المتحدة، حيث تم تحويل إتجاه أربع طائرات نقل تجارية ووجهت لتصطدم بأهداف محددة نجحت في ذلك ثلاث منها، وكانت العواقب أليمة.

تمديده مرتين ولا يزال سارياً في الوقت الحالي. يسمح هذا القانون الوطني للإدارة الأمريكية بالوصول في أي وقت ومن دون إذن قضائي إلى بيانات الكمبيوتر الخاصة بالشّركات أو الأفراد الذين لديهم صلة، أيّاً كانت، مع الولايات المتحدة الأمريكية. في الواقع، هذا الأمر يمكن أن يشكل مشاكل خطيرة للشركة التي تقوم بتخزين بياناتها السّرية والبيانات الشّخصية لموظفيها وعملائها أو بيانات موكليها مثلاً في شركة تزويد حوسبة سحابية أميركية حتى لو كانت فرعاً محلياً لها.

لكن هذا القانون لم يكن أول قانون لوضع معايير الحصول على البيانات لكنه جاء ليعزز المعايير الموجودة من خلال gag Orders أي الأوامر بالتكتم، خاصة في الـ FISA Orders [180] والـ Letters National Security.[181]

سمح هذا القانون في أحد بنوده الحد من السّرية المطلوبة عادةً، من خلال تمكين مزودي خدمة المحمول أو الاتصالات الالكترونية أن يعلنوا أن الـ FBI سعت للوصول إلى معلومات معينة أو حصلت عليها إلّا إذا قررت الـ FBI خلاف ذلك.

ومثالاً على ذلك، في 2014/04/25، أصدرت المحكمة الفيديرالية في نيويورك حكماً بشأن طلب إلغاء جزئي لمصادقة تفتيش ومصادرة، صادرة بحق Microsoft، أجبر هذا الأخير على نقل محتويات رسائل أحد زبائنه. وخصوصية هذه الحالة تكمن في أن هذه الرسائل كانت مخزنة على خوادم موجودة في Ireland. رفضت المحكمة هذا الطلب لأن المصادقة كانت تستهدف Microsoft وهي شركة أمريكية تتحكم في حسابات البريد الالكتروني المستهدفة وتحتفظ بها. استؤنف القرار وأكد عليه في الاستئناف، ومن ثم استئنف الحكم للدائرة الثانية ما يسمى "2nd circuit court" ولجنة من المحكمة عكست رفض الاقتراح لكونه خارج الحدود وغير مصرح به في التصريح الأول. عندها، في 2018/03/23، قام الرئيس الأميركي بالتوقيع على Clarifying Lawful Overseas Use of Data Act (CLOUD Act)، هذا القانون يعدل قانون Stored Commnucation 18 U.S.C §2701 et seq. بإضافة التالي:

"A provider of electronic communication service or remote computing service shall comply with the obligations of this chapter to preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's

---

[180] FISA Orders :Foreign Intelligence Surveillance Act 1978.

[181] Mathias (Cabinet d'avocats): "**Patriot Act: Enjeux, Cloud Computing et Accés aux données**", 2015, published on avocats-mathias.com. (Available on: http://www.avocatsmathias.com/wp-content/uploads/2015/01/LB-VF-Patriot-Act-Mathias-Avocats.pdf) (Accessed on September 16, 2018 at 8:41 AM).

possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States."[182]

أي أن مقدم الخدمة يتحمل التزامات هذا الفصل لحماية محتويات أي اتصال سلكي أو إلكتروني وأي معلومات أخرى أو الكشف عنها، بغض النظر عما إذا كان مثل هذا الاتصال أو السّجل أو أي معلومات أخرى موجودة داخل أو خارج الولايات المتحدة.

وبعد ذلك بفترة وجيزة، حصلت الحكومة، بموجب القانون الجديد على تصريح جديد يغطي المعلومات الناقصة في المذكرة السّابقة. ولكن بتاريخ 2018/03/30، تحركت وزارة العدل لإسقاط الدعوى ووافقت Microsoft على هذا الاقتراح، وبقيت هذه القضية محور جدل كبير.[183]

وبالتالي الولايات المتحدة تحاول بشتى الطرق خرق سيادات الدول والوصول إلى البيانات الموجودة داخلها والحصول عليها، فقانون CLOUD Act الذي أقر 2018/03/23 والذي أتى متمماً ومعدلاً لقوانين سابقة باءت بالفشل، يهدف إلى توضيح القواعد المتعلقة بمتطلبات السّلطات الأمريكية بشأن البيانات المخزنة خارج أراضيها، وهذا يطرح تساؤلاً حول حماية واحترام الحياة الخاصة للأشخاص.[184]

بالرغم من صفحاته العديدة إلّا أنه يتمركز حول فكرتين أساسيتين:

1. أولاً، ينص على أن أي شركة أمريكية –بالمعنى المقصود في القانون الأمريكي، أي كل شركة مسجلة في الولايات المتحدة، وكذلك الشّركات التي تسيطر عليها– يجب أن تكشف للسلطات الأمريكية، بناء على طلبها، بيانات الاتصالات الموضوعة تحت سلطتها بغض النظر عن مكان تخزين هذه البيانات.
2. ثانياً ينص على إمكانية قيام حكومة الولايات المتحدة بالتوقيع على اتفاقيات دولية مع حكومات أجنبية تسمح للسلطات المعنية في كل دولة أن تطلب مباشرة الاتصال الالكتروني ومعالجتها

---

182 CLOUD Act §103(a)(1), Available on: https://epic.org/privacy/cloud-act/cloud-act-text.pdf. (Accessed on September 16. 2018 at 9:32 AM).

183 Supreme Court of the U.S. No. 17-2: United States, Petitioner v. Microsoft Corporation, On Writ of Certiorari to the U.S.Court of Appeals for the Second Circuit, April 17, 2018. (Available on: https://supreme.justia.com/cases/federal/us/584/17-2/) (Accessed on September 12, 2018 at 12:09 PM).

184 Jules-Henri Gavetti: "**le CLOUD Act, une nouvelle loi qui renforce l'ingérence des autorités américaines sur les opérateurs de CLOUD des US**", publié sur : lesechos.fr. (Valide sure: https://www.lesechos.fr/idees-debats/cercle/cercle-181295-le-cloud-act-une-nouvelle-loi-qui-renforce-lingerence-des-autorites-americaines-sur-les-operateurs-de-cloud-des-us-2167111.php) (Consulté le 13 September, 2018 à 08:16 AM).

وتخزينها للبيانات الخاضعة للولاية القضائية للولايات المتحدة، دون الحاجة إلى الذهاب من خلال إجراءات أطول أو خطابات الإنابة القضائية.[185]

وبالتالي مجرد إبرام الاتفاقية الثنائية يسمح بطلب البيانات بدون حاجة إلى الحصول على إذن قضائي ولا يكون خرقاً لسيادة الدولة التي توجد فيها البيانات. ولكن هل هناك على الصّعيد اللّبناني والأوروبي قوانين لمنع السّلطات الأمريكية من الحصول على المعلومات والبيانات الموجودة فيها؟ وهذا ما سنتكلم عنه لاحقاً عند التكلم عن الحق في الخصوصية.

النبذة الثالثة: الوصول القانوني

نص القانون رقم 2018/81 أنه يتوجب على مقدم الخدمة التعاون مع القضاء المختص ووزير الدفاع الوطني ووزير الخارجية بعد موافقة رئيس مجلس الوزراء[186] وضمن حدود صلاحياتهم لإظهار الحقيقة في كل تحقيق يجريه أو في كل دعوى عالقة أمامه.

فللقضاء المختص والمراجع الأخرى المذكورة وضمن حدود صلاحياتهم، في إطار تحقيق أو دعوى، الحق في أن يُلزموا مقدم الخدمات التقنية بتسليمهم البيانات التي في حوزته أو الموضوعة تحت رقابته.

كذلك على مقدم الخدمة أن يزوّد هذه الجهات بحركة البيانات والبيانات التقنية ويخوّلها الوصول إلى المعلومات وفقاً للوقت الحقيقي لأي عملية اتصال عابرة عبر شبكته.[187]

وحركة البيانات هي تلك المتعلقة بجميع الأشخاص الذين يستعملون خدماتهم، والتي تمكّن من تحديد هوية هؤلاء[188]، ويمكن أن تزوّد هذه البيانات وذلك بناءً لطلب من الضابطة العدلية بعد إعلام المرجع القضائي المختص في إطار إجراءات تحقيق في دعوى جزائية ولمدة 30 يوماً على أن تكون هذه البيانات تتعلق بواقعة محددة وأشخاص محددين وذلك بالنظر إلى طابع العجلة وإمكانية تعرّض هذه البيانات للفقدان أو للتعديل.[189]

بالإضافة إلى حالة معالجة البيانات ذات الطابع الشّخصي التي عرّفها قانون 2018/81 أنها كل عملية أو مجموعة عمليات تقع على هذه البيانات مهما كانت الوسيلة المستخدمة، لاسيما عمليات التجميع

---

[185] Simon Dumontel: "**Faut-il avoir peur du CLOUD Act ?**", 25 JUIN 2018, publié sur: august-debouzy.com. (Valide sur : https://www.august-debouzy.com/en/blog/1193-faut-il-avoir-peur-du-cloud-act) (Consulté le september 12, 2018 à 15:49 PM)

[186] المادة 9 من القانون رقم 99/140 الذي يرمي إلى صون الحق بسرية المخابرات التي تجري بواسطة أية وسيلة من وسائل الاتصال.

[187] المادة 76 من القانون رقم 2018/81.

[188] الفقرة الأولى من المادة 72 من القانون رقم 2018/81.

[189] الفقرة الثانية من المادة 72 من القانون رقم 2018/81.

والتسجيل والتنظيم والحفظ والتكييف والتعديل والاقتطاع والقراءة والاستعمال والنقل والنسخ والنشر والمحو والاتلاف وكل شكل آخر لوضع المعلومات تحت التصرف.

بالتالي معالجة البيانات (data processing) هي كل عملية تهدف إلى تحويل البيانات إلى معلومات مفهومة ومنظمة يمكن للشخص الإستفادة منها.

ولكن حدد القانون 2018/81 أنه يجب أن تجمع هذه البيانات بأمانة ولأهداف مشروعة ومحددة وصريحة، ويجب أن تكون ملائمة، غير متجاوزة للأهداف المعلنة، صحيحة، كاملة، ميّومة بالقدر اللّازم.[190] حفظ هذه البيانات لا يكون مشروعاً إلّا خلال الفترة المبينة في التصريح عن المعالجة أو في القرار الذي يرخص بها.[191]

كما يجب إعلام صاحب البيانات بهوية المسؤول عن المعالجة أو هوية ممثله، أهداف المعالجة، الطابع الإلزامي أو الإختياري للإجابة على الأسئلة المطروحة، النتائج التي قد تترتب على عدم الإجابة، الأشخاص الذين سترسل إليهم البيانات وحق الوصول إلى المعلومات وتصحيحها والوسائل المعدة لذلك.[192]

بالرغم من محاولة القانون حماية حق الشّخص الذي تجمع عنه البيانات وإعطاءه حق الإعتراض على المعالجة إلّا أنه عاد وأعفى من موجب الإعلام كما وضع استثناءات على حق الاعتراض:

- الفقرة الثانية من المادة 89: يسقط موجب الإعلام عندما يكون الشّخص المعني على علم بالأمر أو عندما يكون إعلامه مستحيلاً أو يتطلب مجهوداً لا يتناسب مع المنفعة من الإجراء.

لقد ترك المشرع باب التملص من الإعلام واسعاً إذ يمكن للمعالج التذرع باستحالة الإعلام أو حتى بتطلب الإعلام مجهوداً لا يتناسب مع المنفعة من الإجراء، فما هي هذه المنفعة التي تتطلب مجهوداً من المعالج بالحصول على ترخيص بالجمع ومن ثم معالجة بيانات تتعلق بشخص وعدم قيامه بالجهد الكافي لإعلام المعني بالمعالجة. إن عدم تحديد القانون لحالات عدم الإعلام يترك علامة استفهام كبيرة.

- الفقرة الثانية من المادة 92: إلّا أنه لا يحق للشخص ممارسة حق الاعتراض في الحالتين التاليتين:
  1. إذا كان المسؤول عن معالجة البيانات ملزماً بجمعها بمقتضى القانون.
  2. إذا كان قد وافق على معالجة البيانات ذات الطابع الشّخصي الخاصة به.

وضعت مسألة معالجة البيانات في يد سلطة تنفيذية واحدة، فنصت المادة 95 على أنّ كلّ من يرغب بجمع البيانات ذات الطابع الشّخصي ومعالجتها ملتزم بإعلام وزارة الإقتصاد والتجارة بموجب

---

[190] الفقرة الأولى والثانية من المادة 87 من القانون 2018/81.

[191] المادة 90 من القانون 2018/81.

[192] المادة 88 من القانون 2018/81.

تصريح وفق الأصول لقاء إيصال، ولكن هل هذه الوزارة مؤهلة لاستلام مهام مماثلة؟ هل لديها موظفون مؤهلون ولديهم الخبرات اللّازمة لاستلام هذه الوظيفة؟ هل وضعت الأصول اللّازمة للإعلام؟ أوليس التعبير "إعلام وزارة الاقتصاد والتجارة" فضفاض لدرجة التذرع بمجرد الإعلام وعدم أخذ الموافقة وعدم إعطاء الوزارة الحق برفض التصريح؟

كما إن إعطاء هذه الوزارة الحق بتحديد المتطلبات، ما يمنحها سلطة تحديد "الأشخاص الثالثين أو فئاتهم المخولين الاطلاع على البيانات"[193] فيمكنها التعسف باستعمال هذا الحق.

كما ويسمح لعدد من الوزارات بإعطاء هذه التصاريح، كوزارة الداخلية والدفاع، فالمادة 97 تمنح الوزارتين إعطاء ترخيص للبيانات المتعلقة بـ "الأمن الخارجي والداخلي" من دون تعريف للمصطلح. بالإضافة إلى التصريح من وزارة الصّحة في الحالات الصّحية أو بالهوية الجينية أو بالحياة الجنسية، ووزارة العدل في الدعاوى القضائية بمختلف أنواعها.

أعطى بيار الخوري[194] رأيه لـ "SMEX" عن هذه المسألة أن كل هذه الأحكام تسمح لأي شركة خاصة تملك علاقات جيدة مع إحدى هذه الوزارات بالوصول إلى بيانات شخصية حساسة جداً.[195]

كما وإن القانون لم يلزم المسؤولين بإعلام الأشخاص عند اختراق بياناتهم ولكن كل ما نص عليه هو حق المسؤولين بالاعتراض على "الطلبات ذات الطابع التعسفي" لكن لم يحدد ما هو الطابع التعسفي.

كل هذه الأحكام التي نصّ عليها القانون "المنتظر" منذ عدّة سنوات لا تتلاءم مع القوانين والأنظمة الحديثة لاسيما الـ GDPR الذي يوصف بأنه "قانون الخصوصية الأكثر شمولية في العالم". فإذا أردت الحصول على البيانات المتعلقة باللّبنانيين أو القاطنين في لبنان لا داعي للجوء إلى الطرق غير القانونية إذ إن القانون اللّبناني بأحكامه يسمح بالحصول على البيانات بطريقة قانونية بالرغم من عدم وجود حق وذلك لتضنمه مخارج عديدة وعبارات فضفاضة وعدم التحديد والصّرامة. وعليه على المشرع اللّبناني العمل جاهداً لتغيير وتعديل هذا القانون أقله بخلق هيئة متخصصة تهتم بهذه القضايا كما الحال في فرنسا (CNIL) وتونس (INPDP) [196]. فهو يحرم المواطن من السّرية في بياناته التي يتوجب على القانون تعزيز حمايتها.

---

[193] الفقرة الثانية من المادة 98 من القانون 2018/81.

[194] بيار الخوري هو خبير قانوني في مجالات تكنولوجيا المعلومات والاتصالات وحماية المستهلك وعضو اللّجنة النيابية لدراسة مشروع القانون.

[195] https://www.ar.smex.org/ (Accessed on February 28, 2019, at 16:22 PM).

[196] INPDP: الهيئة الوطنية لحماية المعطيات الشّخصية.

الفصل الثاني: الحماية القانونية للبيانات

البيانات المتوجبة الحماية هي عادةً ما تكون البيانات التي تتعلق بالأشخاص أي البيانات الشّخصية فمثلاً إذا عثر أحدهم على USB تحتوي على معلومات يمكن لأي شخص الحصول عليها عن الإنترنت أو في الكتب، فهل تكون هذه المعلومات مستوجبة للحماية؟ هل البيانات المتعلقة مثلاً بحساب مصرفي لأحد الأشخاص تستوجب حماية؟ خاصةً أن الأشخاص يتمتعون بحق منصوص عليه في القوانين معروف بالحق في الخصوصية. فما هو هذا الحق؟ وهل من طرق وأساليب تحميه إلى حدّ ما في ظل الحوسبة السّحابية؟

المبحث الأول: الحق في الخصوصية وتبعاتها

الحق في الخصوصية هو حق شخصي يتعلق بكل فرد على حدة، وتزداد أهمية هذا الحق مع التطور الذي نعيشه يومياً وإختراق التكنولوجيا لهذه الخصوصية بالرغم من العديد من المحاولات للحفاظ عليها. فكيف نظرت القوانين الداخلية والخارجية للحق في الخصوصية؟ وكيف عالجته وحمته؟ هل هناك أساليب جديدة تعزز حماية الحق في الخصوصية؟ وهل واكبت القوانين الداخلية هذه الحاجة في ظل هذا التطور؟

الفقرة الأولى: الحق في الخصوصية

بالرغم من أهمية جميع البيانات المحفوظة على السّحب إلّا إن البيانات ذات الطابع الشّخصي هي التي أخذت غالب اهتمام الدول والقوانين والأنظمة. فلكل إنسان الحق بالتمتع بالخصوصية في ما يتعلق بحياته الخاصة. إن الإعتماد على الوسائط الإلكترونية الحديثة خاصةً خطوط الاتصالات وشبكات الانترنت أدّى إلى خرق الحق في الخصوصية المعلوماتية وهذا الحق من الحقوق الدستورية الأساسية الملازمة للشخص الطبيعي، كذلك من الحقوق التي عولجت ونص عنها في العديد من التشريعات الوطنية والدولية.

النبذة الأولى: حق الخصوصية في القانون اللّبناني

كان الدستور اللّبناني قد كرّس حق الخصوصية في مادته الثامنة التي نصّت على "أن الحرية الشّخصية مصونة في حمى القانون". إلّا أنه ليس هناك مفهوم موحد للحياة الخاصة وهذا الأمر أدّى إلى ترك موضوع التقدير للقضاء. وقد تم تكريس هذا الحق في المادة 12 من الإعلان العالمي لحقوق الإنسان عام 1948 حيث نصّت على أنه "لا يجوز تعريض أحد لتدخل تعسفي في حياته الخاصة أو

في شؤون أسرته أو مراسلاته، ولا لحملات تمسّ شرفه وسمعته. ولكل شخص حقّ في أن يحميه القانون من مثل ذلك التدخل أو تلك الحملات."[197]

قد أقرّ الدستور اللّبناني في مقدمته، إنتماء لبنان إلى منظمة الأمم المتحدة والتزامه بمواثيقها والإعلان العالمي لحقوق الإنسان، ونصّت المادة 14 منه على أن: "للمنزل حرمة ولا يسوغ لأحد الدخول إليه إلّا في الأحوال والطرق المبنية في القانون". ولكن لم يكن يشمل حق الخصوصية سوى ما كان معروفاً عند وضع الدستور (23 أيار 1926) إذ لم يكن متصوراً إتساع نطاق مفهوم الحرية والحياة الشّخصية إلى ما هو عليه اليوم.

إمتداداً إلى القوانين التي لا تقدم ضمانات في ما يتعلق بحماية البيانات الشّخصية سوى بمبادرة جديدة لا تتعدى بضعة أشهر وهي بالقانون المتعلق بالمعاملات الإلكترونية والبيانات ذات الطابع الشّخصي، وبما أن هذه المبادرة مهمّة جداً إلّا أنها تعد خجولة لأن القانون يشمل الكثير من النواقص كما سبق وناقشنا بالأخص في ما يتعلق بحماية البيانات الشّخصية إذ لم يأتِ على ذكر أنواع البيانات فنص فقط على تعريفها بكل ما يعرّف عن شخصٍ.

بالإضافة إلى بعض المواد الواردة في مختلف القوانين السّابقة المتعلقة سواء بحماية البيانات أو الحق بالخصوصية:

1. قانون الحق في الوصول إلى المعلومات الذي كرّس في مادتيه 4 و5 حق الأفراد في الوصول إلى البيانات التي تجمعها الإدارة (الكيانات العامة وعدد محدود من الكيانات الخاصة ولاسيما تلك التي يسيطر عليها كيان ما، أو أي من الأطراف الخاضعة لأحكام القانون المذكور).

   ووفقاً للمادة 4:

أ. يحق لصاحب العلاقة دون سواه الوصول إلى الملفات الشّخصية وأي تقرير تقييمي يتعلق بشخص طبيعي مشار إليه بالاسم أو برقم تعريفي أو بأي وصف تعريفي آخر كبصمات الأصابع أو العين أوالصّوت أو الصّورة.

- يعني بالملفات الشّخصية: قيود الأحوال الشّخصية والملفات التي تتضمن جميع أنواع المعلومات المتعلقة بالشّخص الطبيعي على نحو مباشر أو غير مباشر. بما في ذلك عنوان بروتوكول الانترنت (IP address) وذلك عن طريق مقارنة المعلومات المتعددة المصادر أو التقاطع فيما بينها.

---

[197] نص المادة 12 من الإعلان العالمي لحقوق الإنسان –(http://www.un.org/ar/uniersal-declaration-human-rights/index.html)

ب. يحق لصاحب العلاقة الطلب لتصحيح أو إكمال أو تحديث أو محو المعلومات الشّخصية المتعلقة به غير الصّحيحة أو الناقصة أو الملتبسة أو القديمة أو التي يكون من الممنوع جمعها أو استعمالها أو تبادلها أو حفظها."

وتستبعد المادة 5 مجموعة من المعلومات من المادة السّابقة الذكر غير القابلة للإطلاع بما في ذلك الحياة الخاصة للأفراد، وصحتهم العقلية والبدنية، والأسرار التي يحميها القانون مثل الأسرار المهنية والتجارية.[198]

2. قانون حماية المستهلك الجديد في مادته 58 نص أنه على المحترف الذي يتم التعاقد معه أن يحافظ على المعلومات التي يستحصل عليها وألّا يتصرف بها، ما لم يوافق المستهلك صراحةً على ذلك. كما يتوجب عليه اتخاذ كافة الإجراءات للحفاظ على سريّة هذه المعلومات.

وتخضع الأحكام الواردة في هذا القانون إلى هيئة تعرف بـ "المجلس الوطني لحماية المستهلك" تتبع إجراءات مبسطة تعفي من تعيين محامٍ.

كما أنه يسمح لمنظمات وجمعيات المجتمع المدني أن ترفع شكوى لإبطال البنود التعسفية التي تشملها الشّركات في عقودها.[199]

3. تعاميم مصرف لبنان

ينص التعميم رقم 134 بتاريخ 12 شباط 2015 ما مفاده أن مصرف لبنان ملتزم بـ "حماية المعلومات الشّخصية والمالية للعميل، دون المساس بالقوانين المعمول بها وخاصةً قانون السّرية المصرفية وقانون مكافحة تبييض الأموال وتمويل الإرهاب".[200] كذلك القرار رقم 7548 الصّادر بموجب التعميم رقم 69 بتاريخ 30 آذار 2000 ينص في مادته 12: :بغية الحصول على ترخيص من مصرف لبنان للقيام بعمليات التحاويل النقدية بالوسائل الالكترونية، (...) أن تتقدم بطلب على ثلاث نسخ، واحدة منها أصلية، مرفقاً بها: (...)، 6- المستندات المتعلقة بأنظمة العمل وبالقواعد التقنية التي ستتبعها في تنفيذ عملياتها الالكترونية والتي تثبت أن لديها نظام حماية إلكتروني فعالاً للعمليات التي تجريها...

4. قانون اعتراض الاتصالات رقم 140 بتاريخ 1999/10/27 الذي ينظم اعتراض ومراقبة الاتصالات.

---

[198] المادة 4 والمادة 5 من قانون الحق في الوصول إلى المعلومات رقم 28 الصّادر بتاريخ 2017/02/10.

[199] المواد 58 و67 من قانون حماية المستهلك 659 بتاريخ 5 آب 2004.

[200] Supra 171, p. 7.

5. قانون تنظيم قطاع خدمات الاتصالات رقم 431 بتاريخ 2002/07/22

يفرض هذا القانون بكل بصرامة على كل من يعمل في التفتيش والمراقبة داخل قطاع الاتصالات ألّا يبوح بالمعلومات التي اطّلع عليها في معرض تنفيذه لمهامه إذ إنها تعتبر سريّة، إلّا أنه يمكنه اعلام رؤسائه التسلسليين أو بناء على طلب المرجع القضائي المختص وهذه الأحكام تطبق على كل من اطلع على هذه المعلومات.[201]

6. قانون السّرية المصرفية

بموجب هذا القانون الصّادر في 3 أيلول 1956، لا يحق للبنوك الإفصاح عن الأسرار المصرفية للكيانات الخاصة أو السّلطات العامة، سواء كانت قضائية أو إدارية أو مالية إلّا في الحالات التي يحددها القانون.

7. قانون العقوبات اللّبناني

يعاقب هذا القانون بمــوجب المادة 579 منه كل "من كان بحكم وضعه أو وظيفته أو مهنته أو فنه، على علم بسر وأفشاه دون سبب شرعي أو استعمله لمنفعته الخاصة أو لمنفعة آخر..." وبالتالي السّبب الشّرعي ممكن أن يكون طلب الرؤساء المتسلسلين للموظف فيعفى الفاشي من العقاب، كما ويعاقب كل شخص ملحق بمصلحة البريد والبرق يسيء استعمال صفته للاطلاع على رسالة مختومة أو يتلف أو يختلس إحدى الرسائل أو يفضي بمضمونها إلى غير المرسل، كذلك تفرض عقوبة على من كان ملحقاً بمصلحة الهاتف وأفشى مخابرة هاتفية اطلع عليها بحكم وظيفته أو عمله.[202] كما يعاقب من يتلف أو يفض قصداً رسالة أو برقية غير مرسلة إليه أو يطلع بالخدعة على مخابرة هاتفية.[203]

8. قانون رقم 240 تاريخ 2012/10/22 المعدل لقانون 288 تاريخ 1994/2/22 المتعلق بالآداب الطبية:

يؤكد هذا القانون بالمادة السّادسة منه على أن السّرية المهنية المفروضة على الطبيب هي من النظام العام إلّا أن هذه السّرية تخضع لاستثناءات تحددها القوانين.

كما ونصت المادة 39: "– على الطبيب المولج بالمراقبة الطبية في إدارة ما الاحتفاظ بسر المهنة عند اطلاعه على الملف الطبي سواء بحضور الطبيب المعالج أو بموافقته المسبقة والاكتفاء بإعطاء المعلومات التي لها علاقة أو فائدة من الناحية الإدارية دون تبيان الأسباب الطبية لذلك.

---

[201] المادة 38 من القانون 2002/431.

[202] المادة 580 من قانون العقوبات اللّبناني.

[203] المادة 581 من قانون العقوبات اللّبناني.

- (...) يحظر على الطبيب المراقب إعطاء المعلومات الطبية المدونة في الملفات الطبية إلى أشخاص ثالثين أو لأية إدارة إلّا إذا نصت القوانين العامة أو وافق المريض المعني شخصياً على ذلك."

توفر هذه المواد ضمانات قانونية صلبة فيما يتعلق بالمعلومات الطبية الفردية. ولكن هذه القوانين تعجز أمام التطور التكنولوجي، فتلتزم المستشفيات والأطباء تطبيق معايير واضحة لحماية المرضى من أي اختراق إلكتروني، خاصةً من قبل شركات التأمين التي يهمها الإختراق للاستفادة من المعلومات عن الحالة الصّحية للمرضى واستغلالها في عملها. كل هذه القوانين تنص على الحق بالخصوصية، ولكن هل يمكن التذرع بها والاحتماء تحت أحكامها عندما تكون هذه البيانات على السّحابة التي يطرح حولها العديد من الأسئلة حول الحماية والتي نناقشها في هذه الرسالة بالأخص أن القانون المتعلق مباشرةً بالموضوع تشوبه النواقص؟

النبذة الثانية: حق الخصوصية في الولايات المتحدة والإتحاد الأوروبي

تتخذ الولايات المتحدة والإتحاد الأوروبي أساليب مختلفة تماماً للخصوصية. في الولايات المتحدة، تكون معظم قوانين الخصوصية خاصة بقطاع معين وقد تتفوق مخاوف الخصوصية على مصالح مهمة أخرى مثل حرية التعبير والأمن القومي. أمّا في الاتحاد الأوروبي فتعتبر الخصوصية حقاً أساسياً.[204]
قوانين خصوصية المعلومات في الإتحاد الأوروبي أكثر صرامة من القوانين المماثلة في الولايات المتحدة، فيجب على الشّركات الأمريكية في كثير من الأحيان أن تكون أكثر حذراً في ما يتعلق ببيانات العملاء في الإتحاد الأوروبي مما يتطلب القانون الأمريكي. بعض مزوّدي الخدمة قاموا بفصل السّحب الإلكترونية للإتحاد الأوروبي، ووعد عدد كبير من الشّركات باتباع "The Safe Harbor Framework".

تم سن أول قوانين حماية للبيانات الأوروبية في السّبعينات، من ثم اعتمدت اتفاقية حماية الأفراد في ما يتعلق بمعالجة البيانات الشّخصية عام 1981، وسن قانون حماية البيانات في الاتحاد الأوروبي 95/46 في 1995 (EU Data Protection Directive DPD). يركز الـ DPD 95/46 على حماية البيانات الشّخصية، ومن ثم صوّت على General Data Protection Regulation (GDPR) في كانون الأول من عام 2015، ولكن دخل حيّز التنفيذ عام 2018.
ما هو The Safe Harbor Framework؟

---

[204] Lanois, P. (2010): "**Caught in the clouds: the web 2.0, cloud computing, and privacy?**", Northwestern Journal of Technology and Intellectual Property 9, p. 29.

DPD 95/46 يسمح بتحويل البيانات فقط إلى البلدان الأخرى التي تتمتع بقوانين الحماية المناسبة[205].
لا تملك الولايات المتحدة قوانين خصوصية كافية ولكن يمكن نقل بيانات المستخدمين الأوروبيين إلى الولايات المتحدة إذا كانت الشّركة المزوّدة تتوافق مع الشّروط المفروضة مع الـ SHF بين الولايات المتحدة والإتحاد الأوروبي، وبالتالي إنها إتفاقية تسمح بنقل البيانات من الـ UE إلى الـ USA إذا راعت الشّركة الأمريكية بنود الـ SHF.
يسمح الـ SHF للشركات بالتصديق على الإمتثال لمعايير الخصوصية الأوروبية دون الحاجة إلى استخدام السّحب المعزولة بموجب مبادئ خصوصية الـ SHF، يجب على المنظمات:

1. تقديم إشعار حول جمع البيانات
2. منح الأفراد خيار الإنسحاب (opt out)(أو الإشتراك opt in)، إذا كانت المعلومات الشّخصية تعتبر حساسة.
3. تمديد هذه المعايير نحو التأكد من أن الأطراف الثالثة التي يتم نقل المعلومات الشّخصية الخاصة بها تلتزم أيضاً بمبادئ خصوصية الـ SHF أو تكون لها ضوابط مماثلة
4. تزويد الأفراد بمعلوماتهم الشّخصية التي تحتفظ بها المنظمة
5. اتخاذ خطوات معقولة لحماية سلامة البيانات
6. توفير تدابير كافية لإنفاذ المبادئ

إن التمسك بمبادئ خصوصية الـ SHF يوفر آلية للشركات في الولايات المتحدة للحفاظ على الوضع القائم من نهج التنظيم الذاتي للخصوصية في حين لا تزال مؤهلة لخدمة العملاء في الاتحاد الأوروبي.[206] إلّا أن هذه الإتفاقية تم إعتبارها غير سارية المفعول بقرار صادر عن محكمة العدل الأوروبية بتاريخ 6 تشرين الأول 2015 بقضية بين Maximillian Schrems v Data Protection Commissioner، حيث ماكسيليان المواطن النمساوي الذي يستخدم موقع FaceBook منذ عام 2008، تقدم بشكوى أمام السّلطات المشرفة النمساوية إذ إن القانون وممارسات الولايات المتحدة لا توفر حماية كافية ضد مراقبة السّلطات العامة للبيانات المنقولة إلى ذلك البلد. بالرغم من رفض السّلطات المشرفة الشّكوى معتبرةً أنه تحت إطار SHF توفر الولايات المتحدة الحماية اللّازمة. بعد رفع الدعوى أمام محكمة العدل، رأت هذه الأخيرة أن وجود قرار للجنة يخلص إلى أن دولة ثالثة تضمن مستوى كافٍ من حماية البيانات الشّخصية المنقولة لا يمكن أن يلغي أو يقلل من الصّلاحيات المتاحة للسلطات

---

[205] Stylianou, K.K. (2010): "**An evolutionary study of cloud computing services privacy terms**", John Marshall Journal of Computer and Information Law 27, p. 593.

[206] Carol M, Hayes and Jay P. Kesa: "**Privacy, Law, and Cloud Services**", published in **Encyclopedia of Cloud Computing**, John Wiley & Sons Ltd., United Kingdom, 2016, p. 250.

الإشرافية الوطنية بموجب ميثاق الحقوق الأساسية للإتحاد الأوروبي. فاعتبرت أن قرار اللّجنة غير صحيح، ومن ثم بدأت البحث إذا كانت الإتفاقية بحد ذاتها صحيحة فاعتمدت دراسة خطة عملها. لاحظت المحكمة أن مخطط العمل ينطبق فقط على تعهدات الولايات المتحدة التي تلتزم بها وأن السّلطات العامة للولايات المتحدة ليست خاضعة له. علاوة على ذلك، تسود متطلبات الأمن القومي والمصلحة العامة وإنفاذ القانون في الولايات المتحدة على هذا المخطط بحيث تتجاهل قواعد الحماية المنصوص عنها إذا كانت تتعارض مع هذه المتطلبات. فاعتبرت المحكمة أن هذه الإتفاقية غير سارية المفعول وأبطلتها لتعارضها مع مبدأ احترام الحياة الخاصة. وبالتالي هذا القرار أجبر السّلطات النمساوية على النظر إلى شكوى السّيد "شريمز" والنظر إذا كانت الولايات المتحدة تلتزم بالحماية اللّازمة المنصوص عنها في أنظمة الإتحاد الأوروبي[207].

كذلك الـ GDPR يمنع دول أخرى من الحصول على البيانات الموجودة في الاتحاد الأوروبي إلّا بشروط محددة وذلك لمنع الولايات المتحدة من استخدام قوانينها بشكل تعسفي، فنصت المادة 48 منه على أن:

"Toute decision d'une jurisdiction ou d'une autorité administrative d'un pays tiers exigeant d'un responsable du traitement ou d'un sous-traitant qu'il transfère ou divulgue des données à caractère personnel ne peut être reconnue ou rendue exécutoire de quelque manière que ce soit qu'à la condition qu'elle soit fondée sur un acord international, tel qu'un traité d'entraide judiciaire, en vigueur entre le pays tiers demandeur et l'Union ou un Etat membre, sans préjudice d'autres motifs de transfert en vertu du présent chapitre. »

يجب أن يكون هناك قرار صادر عن سلطة قضائية وإدارية لبلد آخر ويجب أن يكون هناك قرار إتفاقية دولية مثل معاهدة المساعدة القانونية المتبادلة بين البلد الطالب والإتحاد الأوروبي أو دولة عضو.

إضافةً إلى تعزيز حماية البيانات الشّخصية، بالأخص فيما خصّ الـ cookies، إنها لم تأتِ على ذكر هذا المصطلح سوى مرّة واحدة ولكن تداعياتها مهمة للشركات التي تستخدمها لمراقبة عادات تصفح المستخدمين، فنص الـ GDPR في Raison 30 على:

"Les personnes physiques peuvent se voir associer [...] des dentifiants en ligne tels que des adresses IP et des témoins de connexion (« cookies ») ou

---

[207] Maixmillian Schrems v Data Protection Commissioner Judgment in Case C-362/14. (Available on: https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf, Accessed on 18 July 2019).

d’autres identifiants […]. Ces identifiants peuvent laisser des traces qui, notamment lorsqu’elles sont combinées aux identifiants uniques et à d’autres informations recues par les serveurs, peuvent servir à créer des profils de personnes physiques et à identifier ces personnes ».[208]

تعزز هذه المعلومات Raison 26 التي تنص على أن أي معلومات يمكن استخدامها لتحديد شخص ما بشكل مباشر أو غير مباشر تعتبر بيانات شخصية ومن أجل الامتثال، سيتوجب عل الشّركات التوقف عن جمع ملفات الـ cookies أو العثور على سبب شرعي لجمع ومعالجة هذه البيانات. لا تزال معظم الشّركات تعتمد بشدّة على الموافقة (ضمنياً أو عدم المشاركة) على الرغم من أن تعزيز متطلبات GDPR يعني أن الحصول على الموافقة الشّرعية سيكون أصعب بكثير.[209]

فتمت مناقشة هذه المواد في La Loi Cookies إذ إن:

- الموافقة الضمنية لم تعد كافية، يجب تقديم الموافقة عبر إجراء إيجابي مثل وضع علامة مربع قبول أو اختيار إعدادات أو تفضيلات عبر قائمة الإعداد. لا يعتبر مجرد زيارة موقع بمثابة موافقة.
- لا تعد الرسائل، مثل "عند استخدام هذا الموقع، تقبل سياسة ملفات تعريف الارتباط" كافية

(En utilisant ce site, vous acceptez notre politique de cookies)

- يجب أن يكون سحب الموافقة أمراً سهلاً بقدر ما هو مطلوب منحه.
- يجب أن توفر المواقع خيار إلغاء الإشتراك.[210]

---

[208] Raison 30 EU RGDP, valide sur: www.privacy-regulation.eu/fr/r30.htm. (Consulté le 14 Septembre 2018 à 12:00 PM).

[209] Sophie Meunier: "**Comment le RGDP affecte-t-il les politiques de cookies?**", 10 octobre 2017, publié sur : itgovernance.eu. (Valide sur: https://www.itgovernance.eu/blog/fr/comment-le-rgdp-affecte-t-il-les-politiques-de-cookies) (Consulté le 15 Septembre 2018 à 14:47 PM).

[210] Richard Beaumont: "**GDPR Compliance Means Cookie Notices Must Change**", November 3, 2016, published on cookielaw.org. (Available on: https://www.cookielaw.org/blog/2016/11/3/gdpr-compliance-means-cookie-notices-must-change/) (Accessed on September 16, 2018 at 11:25 AM).

الفقرة الثانية: الحق في النسيان

"الحق في النسيان" هو حق كرّسته قوانين أجنبية، وطبقته في النطاق التي لها سلطة عليه، إلّا أن هذه الدول سعت في العديد من الأحيان إلى تمديد نطاق تطبيقه إلى خارج الحدود التي تختص بها وواجهت معارضة من دول أخرى. يجب أولاً فهم ماهية هذا الحق وكيفية تطبيقه، هل هو من الحقوق الأساسية في الحياة السّيبرانية؟ كما وسنتطرق إلى نطاق تطبيقه في ما بعد.

النبذة الأولى: ماهية الحق في النسيان

نتكلم عن "الحق في النسيان" أو المعروف في اللّغة الفرنسية "Droit à l'oubli" أو في اللّغة الإنكليزية "The Right To Be Forgotten" (RTBF) لتسمية الإدعاءات المشروعة للشخص لمحو رؤية معلومات حول ماضيه من سيرة حياته الحالية على الانترنت. في الأساس، لا يقتصر le droit à l'oubli على نطاق الانترنت، فكانت تختلط فكرة هذا الحق مع فكرة مرور الزمن.[211] ولكن في نطاق المعلوماتية، يسمى هذا الحق أحياناً "droit à l'oubli numérique".

في الماضي لم يكن هناك قوانين ونصوص تنص على droit à l'oubli و droit de déréférencement، ولكن اليوم هناك نص المادة 17 من RGDP المعنونة بـ Droit à l'effacement ("droit à l'oubli") والتي تنص على حق الشّخص بطلب إزالة البيانات والمعلومات الشّخصية المتعلقة به وتنص على أسباب طلب الإزالة وعلى الاستثناءات.

في هذا الإطار، يمكننا ذكر القضية المعروفة "Google Spain" بتاريخ 13 أيار 2014، التي بدأت عام 2010 حين تقدم مواطن من الجنسية الإسبانية مع الوكالة الإسبانية لحماية البيانات (AEDP) بدعوى ضد رئيس تحرير صحيفة واسعة الانتشار في اسبانيا، وكذلك ضد Google Spain و Google Inc. وكان السّبب بأنه عندما قام مستخدم انترنت بإدخال إسمه في محرك البحث Google، أظهرت قائمة النتائج روابط لصفحتين من الصّحيفة بتاريخ كانون الثاني وآذار 1998. هذه الصّفحات تنص على الإعلان عن مزاد بيع عقارات وذلك لإيفاء ديونه. يطلب أيضاً من ناشر الصّحيفة إمّا حذف أو تعديل الصّفحات لكي لا تظهر بياناته الشّخصية. ومن ناحية أخرى، يطلب من Google Spain أو Google Inc. حذف بياناته الشّخصية بحيث لا تظهر بعد اليوم بين نتائج البحث والروابط. فتأكدت المحكمة من أن البيانات يتم معالجتها على هذا الخادم وبالتالي تكوّن بيانات شخصية، كذلك تأكدت المحكمة من كون طالب الحذف يتمتع بحق النسيان لأنه عندما تكون معلومات شخص ما مباحة أمام

---

[211] Boizard Maryline: "**Le Droit à l'Oubli, Recherche réalisée avec le soutien de la Mission de recherche Droit et Justice**", faculté de droit et de science politique Rennes 1, février 2015, page 29.

العالم بأسره بمجرد وضع اسمه في محرك البحث، يكون خرقاً للحياة الخاصة وخصوصية الشّخص. كذلك بالنسبة لحرية الإعلام، يجب الأخذ بعين الاعتبار الحياة الشّخصية والرأي العام في آنٍ واحد. ومنذ تاريخ 29 أيار 2014، امتثلت Google لهذا القرار من خلال اقتراح نموذج عبر الانترنت لجمع طلبات حذف نتائج البحث. يجب أن يحدد الطلب مقدم الطلب وعنوان أو عناوين (URL) الروابط المراد إزالتها.[212]

كما ويمكننا ذكر حكمين صادرين عن المحكمة الابتدائية في باريس في 24 تشرين الثاني 2014 و19 كانون الأول 2014، اللّذين ألزما Google بمسح روابط خلافية بعد أن حاولت التوفيق بين الحق في احترام الحياة الخاصة مع حق المعلومات العامة (droit d'information du public).

مع ذلك، صدر حكم عن المحكمة الابتدائية في باريس في 23 آذار 2015، رفض طلب حذف مقال نشر على الانترنت على الموقع الالكتروني لصحيفة يومية باسم حرية المعلومات وفي غياب إساءة استخدام حرية الصّحافة. في هذا الحكم، اتخذت عكس قرار حكميّها السّابق ذكرهما اللّذين أعطيا أولوية للحق في النسيان، ولكن في هذا القرار سعت المحكمة إلى تحقيق توازن عادل بين حريات التعبير والمعلومات وحماية الخصوصية والبيانات الشّخصية، مما يظهر أن الحق في النسيان مرتبط بشروط متعلقة بكل حالة.[213]

من الأحكام الحديثة في آب 2018 التي صدرت للمرة الأولى في Finland والتي تؤكد ترسيخ هذا الحق وانتشاره، تتعلق برجل أدين بجريمة قتل، يطالب بحقه بالنسيان وحذف بياناته الشّخصية عن الانترنت إذ إنها لا تؤثر ولا تعتبر انتهاكاً لحق الجمهور في الوصول إلى المعلومات حول أشخاص مهمين. قدم أمين المظالم (Ombudsman) لحماية البيانات في فنلندا طلب إزالة البيانات لأن Google رفضت إزالة معلومات الرجل عند أول طلب. وجدت المحكمة أن المعلومات التي تظهر تقلص مسؤوليته بالقتل لأسباب صحيّة حسّاسة وخاصة تغلب حق الجمهور بالعلم، فهذا الحق يتمتع بحماية الحق بالخصوصية. سيلزم هذا القرار Google بمسح هذه المعلومات من نتائج محرك بحثها.[214]

---

[212] Lamia El BADAWI, Le droit à l'oubli à l'ère du numérique, LA REVUE, « le droit à l'oubli » Numéro 8, Septembre 2016, p. 21-23.

[213] Ibid, page 25.

[214] Yle: "**Finnish court issues precedent "right to be forgotten" decision for Google to remove data**", published on yle.fi, August 17, 2018. (Available on: https://yle.fi/uutiset/osasto/news/finnish_court_issues_precedent_right_to_be_forgotten_decision_for_google_to_remove_data/10358108) (Accessed on September 22, 2018 at 10:08 AM).

يمكننا الاستنتاج أن الحق في النسيان يشتمل على عنصرين: الحق في المسح أو الشّطب droit à l'effacement والحق في الإزالة من قائمة المراجع droit au déréférencement. الحق في المسح هو حق الشّخص في أن يزيل محتوى الشّبكة الإلكترونية التي قد تضر به، يمكن أن يكون مقالة إخبارية أو صورة أو فيديو أو أي منشور يمس حياته الشّخصية، سواء أكان ذلك على مواقع التواصل الإجتماعي أو على موقع الصّحافة على الانترنت أو في أي مساحة للتعبير الرقمي، فيمكن حذف المعلومات التي تهم الطالب.

أمّا بالنسبة إلى حق الإزالة من قائمة المراجع، فهو يتكون من استبعاد بعض مصطلحات محركات البحث والتي سيتم استبعادها من نتائج البحث في المستقبل. فللإشارة فقط، إن إزالة محتوى لا تؤدي تلقائياً إلى إزالته عن محركات البحث، فرابط الصّفحة المحذوفة يبقى موجوداً في نتائج البحث لفترة معينة من الوقت. إذا كان الرابط لا يزال متاحاً، ومن الممكن أن تظل بعض معلومات الصّفحة ظاهرة، حتى لو كانت قليلة وذلك قد يؤدي إلى فهم المحتوى القديم للصّفحة الذي يكون في بعض الأحيان محرجاً. بالإضافة إلى ذلك، من الممكن الوصول إلى المحتوى من خلال ذاكرة التخزين المؤقت le cache. فما هو le cache؟

أولاً، يجب أن يكون القارئ على دراية أن محرك البحث هو روبوت يحدّث باستمرار قاعدة البيانات الخاصة به: فمن ناحية إنه يسعى إلى دمج صفحات جديدة لا يعرفها لجعلها قابلة للوصول إلى نتائج البحث. من ناحية أخرى، يقوم بتحديث قاعدة البيانات الخاصة به بحيث تتوافق الروابط التي تظهر ذلك، مع محتوى الصّفحة الأساسية.

لتحقيق ذلك، تجعل الروبوتات نسخة من الصّفحة المرجعية للتحقق خلال الزيارة القادمة سواء تم تغييرها بمقارنتها مع الصّفحة الجديدة أم لا. يتوفر هذا الإصدار الأقدم من الصّفحة في عنصر يسمى ذاكرة التخزين المؤقت (cache). فبفضل le cache، يمكن الوصول إلى المحتوى الذي تم تعديله أو حذفه، فالمشكلة تكمن أنه إذا تم حذف شيء من موقع سيكون الوصول إلى المحتوى متاحاً حتى المرور التالي للروبوت. وبالتالي لن يكون صعباً على مستخدم الانترنت الفضولي العثور على محتويات لا يراد ظهورها على الانترنت.[215]

---

[215] Florian Chague: "**Contrôlez l'utilisation de vos données personnelles**", 7 Septembre 2017, publié sur openclassrooms.com.
(Valide sur: https://openclassrooms.com/fr/courses/2807371-controlez-lutilisation-de-vos-donnees-personnelles/3082821-quest-ce-que-le-droit-a-loubli) (Consulté le 19 Septembre 2018 à 09:30 AM).

النبذة الثانية: نطاق تطبيق هذا الحق

إن تطبيق الحق في النسيان خارج الحدود الإقليمية ربما يكون أكثر القضايا الشّائكة التي تنبغي معالجته عند تنفيذه. ولكن كما يقول Professor Floridi:

"Yet I fear that, in an infosphere that does not know geographical boundaries, acting on search engines to block access to contents is never going to be the ultimate solution. If some content is harmful, it should be blocked at the source, for any search engine, anywhere, or removed completely, as we do with child pornography. Only this would be an effective implementation of the right to be forgotten."[216]

أي أنه يخشى أن الحذف عن محركات البحث لن يكون الحل، بل يجب الحذف من المصدر من أي مكان عن أي محرك في العالم وهذا يكون التنفيذ السّليم لتحقيق فكرة الحق في النسيان.

وبالتالي لا يتحقق هذا الحق إذا كان محصوراً فقط في الـ EU ولا تزال المعلومات قابلة للوصول إليها خارج الاتحاد إذا كانت موجودة على خوادم خارجيّة.

وكذلك المؤسسات الأوروبية تصادق على الرأي القائل بأنه يجب أن يكون الوصول إلى القائمة قد تجاوز الحدود الإقليمية. أشارت WP29 Guidelines [217] إلى أنه لا يمكن اعتبار تقييد شطب مجال الاتحاد الأوروبي وسيلة كافية لضمان حقوق أصحاب البيانات بشكل مرضٍ. من الناحية العملية، يعني أن يكون الإلغاء فعالاً في جميع نطاقات ".com" ذات الصّلة.[218]

---

[216] Luciano Floridi: "**We Dislike The Truth and Love to Be Fooled**", CYCEON, November 21, 2016. (Available on: https://cyceon.com/2016/11/21/luciano-floridi-oxford-ukgoogle-interview) [https://prma.cc/6NRN-HTAL] (Accessed on September 17, 2018 at 11:15 AM).

[217] **WP29** هي مختصر لـ Article 29 Working Party وهي هيئة استشارية مؤلفة من ممثل عن هيئة حماية البيانات في كل دولة عضو في الاتحاد الأوروبي، والمشرف الأوروبي والمفوضية الأوروبية. في 25 أيار 2018، تم استبدالها بالمجلس الأووبي لحماية البيانات [European Data Protection Board (EDPB)] بموجب الـ GDPR. تكوين وأهداف الهيئة WP29 تم تعيينه في المادة 29 من الـ DPD وتم العمل بها في عام 1996.

[218] See **Article 29 Data Protection Working Party**, Guidelines on the Implementation of the Court of Justice of the European Union Judgement on "Google Spain and Inc. v. Agencia Espanola De Protection De Datos (AEPD) and Mario Costeja Gonzalez" C-131/12 (2014) [https://www.dataprotection.ro/servlet/ViewDocument?id=1080].

وفقاً لمبادئ WP29 Guidelines، أمرت الهيئة الوطنية لحماية البيانات الفرنسية CNIL، Google بتطبيق حق النسيان على جميع أسماء نطاقات محرك بحث google بما في ذلك نطاق ".com".[219]
مثل عديد من هيئات حماية البيانات الوطنية الأخرى في أوروبا، تشرف CNIL على تطبيق حكم محكمة العدل الأوروبية (ECJ) على الحق في النسيان في حالة رفض محركات البحث تنفيذ الشّطب المطلوب. رداً على مئات من الشّكاوى الفردية منذ قرار Google Spain، طلبت CNIL من Google شطب نتائج البحث في مناسبات متعددة. في كل تلك الحالات، طلبت CNIL صراحةً أن يكون الشّطب فعالاً عبر محرك البحث بأكمله بغض النظر عن امتداد النطاق الذي يصل من خلاله المستخدمون إلى المعلومات. ومع ذلك، في البداية، طبقت Google الشّطب فقط عن المحركات الأوروبية، وظل الوصول إلى نتائج البحث المطلوب نسيانها وحذفها متاحاً في الأراضي الفرنسية من google.com والخوادم الأخرى غير الأوروبية.[220]
كان الحل المقترح من Google هو geo-localization (أي التوطين الجغرافي)، فوسعت Google إزالة عناوين URL. مثلاً إذا طلب أحد المقيمين في فرنسا من Google إزالة نتيجة بحث ضمن طلبات البحث الخاصة باسمه ووافقت Google على ذلك، فلن يكون مرئياً على أي إصدار من موقع Google، بما في ذلك google.com عندما يتم الوصول إلى محرك البحث من فرنسا. تستخدم Google عنوان IP للمتصفح لتحديد الموقع ومع ذلك، فقد اعتبرت CNIL أن هذا التطوير غير كافٍ لحماية حقوق المستخدمين الفرنسيين. لجنة في CNIL لاحظت أن:

“The right to be delisted is derived from the right to privacy, which is a universally recognized fundamental right laid down in international human rights law. Only delisting on all of the search engine’s extensions, regardless of the extension used or the geographic origin of the person performing the search, can effectively uphold this right. The solution that consists in varying the respect for people’s rights on the basis of the geographic origin of those viewing the search results does not give people effective, full protection of their right to be delisted.”[221]

بمعنى أنه يجب شطب جميع إضافات محرك البحث، بصرف النظر عن امتداد المستخدم أو الأصل الجغرافي للشخص الذي يجري البحث.

---

[219] CNIL orders Google to Apply Delisting on All Domain Names of the Search Engine, CNIL, June 12, 2015, https://www.cnil.fr/fr/node/15790 [https://perma.cc/5DP4-7NUV]

[220] Supra 218.

[221] CNIL, Restricted Committee, Decision No. 2016-054, Mar. 10, 2016. (Available on: https://assets.documentcloud.org/documents/2775951/d2016-054-Penalty-Google.pdf) [https://perma.cc/AZA6-6J44] (Accessed on September 17, 2018 at 12:48 PM).

وفقاً لـ CNIL، إن الحق في النسيان هو أمر مطلق يجب على المؤسسات الفرنسية حمايته ما دام التعدي عليه يسبب أضراراً للمواطنين الفرنسيين. كما توضح أيضاً أنه لا يزال بإمكان جهات الإتصال الموجودة خارج أوروبا الوصول إلى نتيجة البحث المشطوبة المرتبطة بالمحتوى الذي قد ينتهك خصوصية الشّخص المعني، وكذلك جهات الاتصال الموجودة في أوروبا عند استخدامها محرك بحث غير أوروبي. يبقى الخيار فقط الامتثال لطلبات CNIL أو التوقف عن تقديم الخدمات في فرنسا. فهناك دعوى أمام المحاكم الفرنسية بين CNIL وGoogle بموضوع الـ extraterritorial، ولكن رأي Google كان أنه لا يجب على EU فرض تطبيق قوانينها المتعلقة بالخصوصية في جميع أنحاء العالم وإذا طُبِقَ سيؤدي إلى خرق سيادة دول أخرى وخرق قوانينها، مثلاً هناك خطر يتمثل في أنه عند تطبيق Google ذلك في الولايات المتحدة، فقد يؤدي إلى التعدي على الحماية المحلية لحرية التعبير.

هذه القضية تظهر أن لكل طرف حجج، كما سبق وذكرنا، فـ CNIL تركز على حماية الحقوق الفردية بينما Google تصرّ على الآثار الاقتصادية والاجتماعية الأوسع.

بتاريخ 11 أيلول 2018، بعد سماع المحكمة للدفوع في هذه القضية، أحال المجلس الفرنسي –الذي يفصل في هذا النزاع على المستوى الوطني في فرنسا – أربعة أسئلة تتعلق بالحكم الأولي إلى Luxembourg:

أولاً: إذا كان المسح بعد الطلب المقبول للحذف يجب نشره في ما يتعلق بجميع أسماء النطاقات بغض النظر عن مكان وجود طالب الحذف حتى لو حدث ذلك خارج الاتحاد الأوروبي.

ثانياً: (إذا كان الجواب على السّؤال الأول سلبياً) إذا كان تطبيق الحق في النسيان يجب أن يتعلق فقط باسم النطاق الخاص بالدولة العضو التي يعتبر أنه قد تم تشغيل البحث فيه،

ثالثاً: إذا كان يجب القيام بذلك في ما يتعلق بأسماء النطاقات المتعلقة بجميع الدول الأعضاء،

رابعاً: إذا كان الحق في النسيان ينطوي على فرض الحظر الجغرافي على مشغلي محركات البحث في حال كان المستخدم موجوداً في:

1. الدولة العضو التي صدر منها طلب الحذف،
2. أراضي مناطق البحث الخاصة بالاتحاد الأوروبي من مجالات غير أوروبية.[222]

[222] First, whether the de-referencing following a successful request for erasure must be deployed in relation to all domain names irrespective of the location from where the search based on the requester's name is initiated, even if that occurs outside of the EU.
Second, if the first question is answered negatively, whether the RTBF must only be implemented in relation to the domain name of the Member State from which the search is deemed to have been operated or, third, whether this must be done in relation to the domain names corresponding to all Member States,
Fourth, whether the RTBF implies an obligation for search engine operators to use geo-blocking where a user based in (i) the Member State from which the request for erasure emanated or (ii) the territory of the EU searchers non-EU domains.

والرد على هذه الأسئلة من المتوقع أن يتم في شهر كانون الأول 2018 والحكم من المتوقع أن يصدر في عام 2019، وهذا الحكم سيؤدي إلى توسيع نطاق تطبيق الحق في النسيان إذا تم المصادقة على مطالب CNIL.[223]

بتاريخ 10 كانون الثاني 2019، تم إعلان رأي المحامي العام Maciej Szpunar الذي يقضي بأنه يجب وضع تمييز على أساس المكان الذي يجري منه البحث. فالبحث الذي يتم من خارج الإتحاد الأوروبي يقع خارج نطاق القانون الأوروبي وبالتالي الشّركة غير مخوّلة إزالة الروابط من نطاق البحث؛ هذا الأمر يضع قيود كثيرة على التأثير الخارجي المحتمل لقانون حماية البيانات الأوروبي. ففي نظر المحامي العام، هذه هي النتيجة المنطقية للإنترنت التي ليس لها حدود جغرافية.

وفقاً له، يجب الموازنة بين الحق في النسيان وحق الجمهور بالوصول إلى المعلومات المطلوبة. إذا كان ينبغي إزالة الروابط في جميع أنحاء العالم، فإن التوجيه EC/46/95 للبرلمان الأوروبي والمجلس المؤرخ 24 تشرين الأول 1995 بشأن حماية الأفراد فيما يتعلق بمعالجة البيانات الشّخصية والحركة الحرّة لهذه البيانات (OJ 1885 I 281, P, 31) لسيوا في وضع يسمح لهم بتحديد وتسجيل الحق في الحصول على المعلومات وحتى بقياس هذا الحق بغيره من الحقوق الأساسية المتعلقة بحماية البيانات واحترام الحياة الخاصة. إذ إن المصلحة العامة في الوصول إلى المعلومات ستختلف حسب الموقع الجغرافي من بلدٍ إلى آخر. إن إزالة الروابط على المستوى العالمي ينشئ خطر أن بلدان ثالثة قد يتم منعها من الوصول إلى المعلومات وهذه البلدان الثالثة، على أساس المعاملة بالمثل قد تمنع الوصول إلى المعلومات من قبل أشخاص في الدول الأعضاء في الإتحاد.

فالمحامي العام ينصح المحكمة بأن تصدر قرار بعدم فرض إلتزام إزالة النتائج على الصّعيد العالمي عند التذرع بالحق في النسيان.

كما يؤكد من ناحية أخرى، أنه بمجرد تأسيس الحق في إزالة الروابط داخل الإتحاد الأوروبي، يجب على مشغل البحث إتخاذ جميع التدابير الممكنة لضمان الإزالة الفعالة والكاملة للروابط داخل إقليم الإتحاد، أيضاً من خلال تقنية geoblocking من عنوان IP الذي يعتبر موجوداً في إحدى الدول الأعضاء، بغض النظر عن اسم النطاق الذي أدخله مستخدم الإنترنت الذي يجري البحث.[224]

---

[223] https://www.law.ox.ac.uk/business-law-blog/blog/2018/11/google-v-cnil-defining-territorial-scope-european-data-protection-law

[224] Bart Van Den Brande: "**Right to be forgotten**" **limited to the EU territory?**, January 17, 2019, published on siriuslegaladvocaten.be.

(Available on: https://siriuslegaladvocaten.be/en/right-to-be-forgotten-limited-to-the-eu-territory/) (Accessed on February 16, 2019 at 10:05 AM).

وهذا الرأي غير ملزم للمحكمة التي لم تصدر قرارها حتى اليوم، ولكنه يعتبر إنتصاراً لشركة Google خاصةً إذا صدر القرار مطابقاً لهذا الرأي.

المبحث الثاني: حل النزاعات القانونية

عند نشوء أي نزاع في السّحابة خاصة في العلاقة ما بين المزوّد والمستخدم في ما يتعلق خصيصاً بتطبيق العقد المبرم بينهما، بغض النظر عن الجرائم التي يمكن أن تقع في إطار السّحابة التي تتطلب دراسة موسعة، يجب دراسة الطرق التي يجب اللّجوء إليها لحل النزاع وتحديد مسؤولية المزوّد وحالات انتفائها.

الفقرة الأولى: طرق حل النزاعات

تختلف طرق حل النزاعات من طرق تقليدية أي الطرق القضائية والطرق الحبية وتتأثر بحسب النزاع الناشئ إذا كان يتعلق بنزاعٍ داخلي أو دولي أو حتى اليوم بنزاعات في الفضاء السّيبراني؛ نرى وجود طرق حل نزاعات إلكترونية. فما هي الوسائل المستخدمة في إطار الحوسبة السّحابية عند وجود أي نزاع؟ وما هو القانون الواجب التطبيق؟

النبذة الأولى: المحاكم المختصة والقانون الواجب التطبيق

كون العقد السّحابي عقد إذعان، فعند إبرامه يضع المزوّد البنود التي تناسبه من ضمنها بند الإختصاص القضائي وطرق حل النزاعات، يختلف هذا البند من مزوّد إلى آخر، فمنهم من يقوم بتحديد القانون والمحاكم المختصة، منهم من يحدد التحكيم كوسيلة لحل النزاع، ومنهم من لا يقوم بتحديد أيّ من ذلك إلّا أن هذه الفئة الأخيرة شبه نادرة.

البند الأول: العقود التي تحدد الإختصاص القضائي

بما أن الحوسبة السّحابية ليست كباقي الخدمات المعلوماتية وليست كاستخدام الانترنت بشكل عادي، وكما ذكرنا سابقاً هناك علاقة تعاقدية تربط بين أطراف العلاقة، فيخضع هؤلاء إلى أحكام هذا العقد. وعليه، يخضع الأطراف إلى المحاكم والقوانين المعينة في العقد. إن الشّركات الكبيرة والأشخاص الحكوميين يمكنهم مفاوضة العقود السّحابية أمّا المستهلكون والشّركات الصّغيرة وجديدة النشأة يخضعون للشروط والأحكام الموضوعة من قبل المزوّد. مثلاً مستهلك أو شركة في لبنان تدفع 100$ للإستفادة من خدمة سحابة حدد في عقدها اختصاص محاكم كاليفورنيا، سينفق المستهلك الأموال الطائلة للحصول على حكم.

إحصاءات عديدة أظهرت أن الشّركات المزوّدة تنص في عقودها على أحد القوانين التالية الواجبة التطبيق:

- قانون إحدى الولايات الأمريكية
- قانون إحدى الدول التابعة للإتحاد الأوروبي
- القانون الكندي
- القانون المحلي للمستهلك
- التحكيم
- لم يذكر العقد أي قانون أو ذكر قانوناً بشكل غامض (مثلاً "UK Law")

وهناك الكثير من القوانين الأخرى التي يمكن أن تكون في عقود سحابية أخرى، كما وهناك الكثير من العقود التي تعدل بين الحين والآخر ويعلن عنها المزودون لذلك على الفرد التأكد من الشّروط ToS بين الحين والآخر.

العديد من هذه الشّركات المزوّدة قد تضع أكثر من قانون حسب المنطقة الجغرافية التي يوجد فيها المتعاقد وتبقى عقود غرر إذ إنها توضع من طرف واحد. فمثلاً:

1. Apple: بحسب تحديث تاريخ 17 أيلول 2018 للاتفاقية بينها وبين مستخدمي سحابتها iCloud، تفرق إذا ما كان المستخدم أميركياً، غير أميركي، أو يعيش في الاتحاد الأوروبي أو سويسرا أو النرويج أو أيسلند.

   إن الذين يعيشون في الإتحاد الأوروبي، سويسرا، النرويج وأيسلند يخضعون إلى قوانين بلدهم؛ أمّا الذين يعيشون في الولايات المتحدة أو خارجها باستثناء من أتينا على ذكرهم، يخضعون لقانون ولاية كاليفورنيا بشكلٍ قاطع لا رجوع عنه بغض النظر عن أي تعارض لأحكام القانون.[225]

2. عقد Google Cloud Platform بحسب آخر تحديث له بتاريخ 27 حزيران 2018 يميز بين الهيئات الحكومية الأميركية والهيئات الحكومية الفيدرالية الأميركية والكيانات الأخرى:

   فبالنسبة للهيئات الحكومية الأميركية على المدينة والمقاطعة والولاية، تلتزم هذه الاتفاقية الصّمت في ما يتعلق بالقانون الواجب التطبيق.

   وبالنسبة للهيئات الحكومية الفدرالية الأميركية تكون خاضعة لقانون ولاية كاليفورنيا (باستثناء قواعد تنازع القوانين) في حالة غياب القانون الفيدرالي المعمول به.

   أمّا بالنسبة للكيانات الأخرى، فتحكم بموجب قانون ولاية كاليفورنيا باستثناء قواعد تنازع القوانين.[226]

---

[225] The Legal Agreement Between "You" And Apple that governs the use of the iCloud product, software and websites.
(Available at: https://www.apple.com/ca/legala/internet-services/icloud/en-terms.html.)

[226] Google Cloud Platform between Google and the user. (Available at: https://cloud.google.com/terms.)

3. شركة Microsoft، تقسم الاتفاقيات المتعلقة بـ Microsoft Cloud وفق المناطق فمثلاً الاتفاقية المتعلقة بلبنان تنص على أنها تخضع لقوانين أيرلندا، أمّا بالنسبة للإختصاص المكاني للمحاكم، فإذا كانت الدعوى مقامة من قبل Microsoft على العميل فيكون الاختصاص لمحاكم المقر الرئيسي للعميل، أمّا إذا أقام العميل الدعوى فيقيمها في أيرلندا. ولا يمنع خيار دائرة الاختصاص هذا أي طرف من السّعي للحصول على الدعم القضائي في أية دائرة اختصاص قضائية ملائمة في ما يتعلق بانتهاك حقوق الملكية الفكرية.[227]

وبالتالي كل عقد يتضمن بنوداً خاصة به وبكل حالة ويجب دراسة كل عقد على حدة.
أمّا بالنسبة للمحاكم المختصة بالنظر في هذه القضايا، فتحدد أيضاً في العقد وتكون متوافقة عادةً مع النظام القانوني المحدد فيه. مثلاً في العقود التي سبق وذكرناها:

1. Apple تحدد اختصاص محاكم SantaClara في كاليفورنيا وبذلك تتطابق مع القانون المحدد. أمّا في ما يتعلق بالذين يعيشون في أي بلد من الإتحاد الأوروبي أو سويسرا أو النرويج أو أيسلند فتكون المحاكم المختصة تلك الموجودة في مكان إقامة الشّخص.[228]

في حالات تحديد الإختصاص في العقد، سمح للمحترفين بالقيام بذلك، ولكن عندما يتعلق الأمر بالمستهلك، فالقانون الوضعي التقليدي الخاص بحماية المستهلك لا يسمح بهذه البنود إذ يعتبرها بنوداً تعسفية وتكون قابلة للإبطال أمام القضاء المختص، حتى أن المشترع اللّبناني يعتبرها باطلة بطلاناً مطلقاً[229]. ولكن ما مدى صحة الإبطال بعد موافقة المستهلك عليها؟
في الأساس لا يجوز للمستهلك التنازل عن حقه بالمقاضاة أمام محاكم دولته قبل نشوء النزاع، فهي من القواعد الآمرة كونها تتعلق بالنظام العام، ولكن يمكنه استعمال حقه بالاختيار بعد وقوع النزاع[230]، إلّا إن اقتراح اللّجنة القانونية الأوروبية بمناسبة وضع التنظيم الأوروبي المتعلق بمنع البنود الاتفاقية المتعلقة بتعيين الاختصاص القضائي سمح بهذه البنود على أن يكون هناك حق اختيار للمستهلك لناحية قبول قانون دولة البائع (المزوّد) أو اللّجوء إلى الطرق غير القضائية.

---

227 Microsoft Cloud Agreement.
(Available at: https://download.microsoft.com/download/2/C/8/2C8CAC17-FCE7-4F51-4D77C7022DF5/MCA2017Agr_EMEA_MEA_EE_ARA_Sep20172_CR.pdf)
228 Supra 225.

229 المادة 26 الفقرة 10 من قانون حماية المستهلك.

230 Olivier Cachard: "La Regulation Internationale Du Marché Electronique", Lgdj, 2002, p. 355-377 et suite.

البند الثاني: العقود التي لا تحدد الإختصاص القضائي

الأمر الذي يثير صعوبة هو عند عدم تحديد القانون والمحاكم المختصة، فكيف يتم اختيار القانون الواجب التطبيق والمحاكم المختصة؟

أولاً، يجب التأكيد على أن العقد الدولي يخضع لمبدأ حرية الأطراف في اختيار القانون. وهذه الفكرة قديمة قد استقر العمل بمبدأ سلطان الإرادة في فرنسا بصدور حكم محكمة النقض الفرنسية في 5 كانون الأول 1910 الذي نصّ على أن "القانون الواجب التطبيق على العقود سواء في ما يتعلق بتكوينها أو آثارها أو شروطها، هو القانون الذي تتبناه الأطراف."[231] كما ويمكن أن يتم الاتفاق على هذا القانون في وقت لاحق من ابرام العقد وهذا ما اتفق عليه الفقه.[232] لكن عدم الإتفاق يطرح مسألة الإختصاص القضائي ومسألة تنازع القوانين. فما هي الحالة في ما يختص بالحوسبة السّحابية؟

في بادئ الأمر يجب التمييز بين حالتين: حالة المستهلك وحالة غير المستهلك أو المحترف. وبما أن المحترف يفاوض في معظم الأوقات على بنود العقد ويمكنه المفاوضة على تعيين الإختصاص القضائي والقوانين التي يريد تطبيقها، فسنبحث فقط في حالة المستهلك عند عدم تحديد قانون وقضاء مختص في العقد.

على القاضي في هذه الحالة أن يعتمد قانون الدولة الأكثر صلة بالعقد عملاً باتفاقية روما، من ثم الإحالة إلى اختصاص قانون محل إقامة المتعاقد المتوجب عليه تقديم العمل الأساسي في العقد أي محل عنوان إقامة المزوِّد المتمركز في الشّركة. كما نصت إتفاقيتا بروكسل (1968) ولوغانو (1988) الأوروبيتان المتعلقتان بالإختصاص القضائي وتنفيذ الأحكام التجارية والمدنية، على إمكانية إقامة الدعوى أمام القضاء في محل تنفيذ الموجب الأساسي أو اقتضاء تنفيذه.[233] وعند انتفاء محل إنشاء العقد ومحل تنفيذه، يعتمد على مؤشرات كشكل العقد ولغته أو جنسية المتعاقدين...

لكن يزداد تعقيد هذه العناصر في النزاعات الناشئة عن علاقة إلكترونية والتي تنشأ بين أطراف من دول مختلفة وعديدة ويتم تنفيذها والدفع بموجبها في دول ثالثة، خاصة عندما يكون النزاع واقعاً بين المستهلك والمحترف إذ إن القوانين الداخلية للدول المتعلقة بحماية المستهلك هي ذات تطبيق إلزامي على تعيين دولة محل إقامة المستهلك.[234]

إن إتفاقية بروكسيل لم تركز في الأساس على حماية المستهلك، لكن تم تمديد نطاق الحماية للمستهلكين من خلال حكم Bertrand v. Ott حيث تم توضيح أن الإتفاقية ستطبق على المستهلكين الذين ستتم

---

[231] خالد عبد الفتاح محمد خليل، حماية المستهلك في القانون الدولي الخاص، دار الجامعة الجديدة للنشر، الإسكندرية، عام 2009 م، ص. 75-76.

[232] هشام علي صادق، تنازع الاختصاص القضائي الدولي، دار المطبوعات الجامعية، الإسكندرية، 2002م.

[233] المادة 5 فقرة أولى من إتفاقية بروكسل لعام 1968 والمادة 5 فقرة أولى من إتفاقية لوغانو لعام 1988.

[234] طوني عيسى: التنظيم القانوني لشبكة الإنترنت، صادر، بيروت، 2001، صفحة 451 وما يليها.

حمايتهم بسبب "ضعفهم مع البائعين"[235]. وأسست هذه الإتفاقية لإتفاقية لوغانو التي تضمنت أحكاماً مماثلة لها، ولكن اتفاقية بروكسيل استبدلت بتنظيم بروكسيل الأول (2001/44) ولكنها بقيت مطبقة على العلاقة بين الاتحاد الأوروبي والدنمارك.

في المادة 14، تحدد اتفاقية بروكسل بوضوح الشّروط المؤيدة لحماية المستهلك، مما يمنح المستهلكين حرية اختيار قضاء أكثر ملاءمة لإجراءاته.[236]

هل من الممكن تطبيق قواعد القانون الدولي الخاص والإتفاقيات والمعاهدات الموجودة على نزاعات الحوسبة السّحابية؟

فمثلاً إذا نظرنا إلى الخدمة السّحابية على أنها علاقة بين مهنيين، Brussels I Regulation تنص على اختصاص محاكم موطن المدعى عليه، وهذا التنظيم يقتصر على الأطراف المقيمين في الدول الأعضاء في الإتحاد الأوروبي، وإذا لم يكن للخدمة السّحابية الموجودة خارج الإتحاد الأوروبي فرع أو وكالة أو مؤسسة أخرى في الإتحاد الأوروبي فإنها تخرج من نطاق Brussels I Regulation.

أمّا بالنسبة للخدمات السّـحابية، يجب أن تكون الشّروط المنصوص عليها في المادة 17(ج)[237] بشأن عقود المستهلك ذات اهتمامات خاصة. اعتماداً على تفسير هذه الشّروط، فإن الخدمات السّحابية تندرج تحت نطاق Brussels I عندما يتعلق الأمر بعقود المستهلك.

في قانون التجارة التقليدية والقانون الدولي الخاص، يكون لموقع الأداء الأكثر صلة بالعقد الاختصاص ولكن في حالة السّحابة، إن موقع نشاط الخدمة مشكوك فيه إلى حد كبير في بعض الأحيان. بينما من الممكن أحياناً وبصعوبة تحديد الخوادم المستخدمة في تقديم الخدمات السّحابية، إذ إن نشاط الخادم يتشتت بسبب تجميع الموارد وسرعة المرونة للحوسبة السّحابية. خاصةً عندما تتعلق بسحابة عامة، من

---

[235] Case 150/77 Bertrand v. Ott [1978] ECR 1431, para 21.

[236] Article 14 of Brussels Convention: "A consumer may bring proceedings against the other party to a contract either in the courts of the contracting state in which that party is domiciled or in the courts of the contracting state in which he is himself domiciled. Proceedings may be brought against a consumer by the other party to the contract only in the courts of the contracting state in which the consumer is domiciled."

[237] Article 17.1.c:"In matters relating to a contract concluded by a person, the consumer, for a purpose which can be regarded as being outside his trade or profession, jurisdiction shall be determined by this Section, without prejudice to Article 6 and point 5 of Article 7, if:

(c) in all other cases, the contract has been concluded with a person who pursues commercial or professional activities in the Member State of the consumer's domicile or, by any means, directs such activities to that Member State or to several States including that Member State, and the contract falls within the scope of such activities."

الصّعب تحديد موقع البيانات التي يتم ترحيلها بين عدّة خوادم لأغراض موازنة الحمل أو قد يتضمن الموقع عدّة خوادم في نطاقات قضائية مختلفة لخدمة معينة خلال فترات زمنية قصيرة. في حالات معينة، يتم تحديد الموقع والاختصاص القضائي للخوادم في الشّروط والأحكام. إن بعض مستخدمي السّحابة يصرّون على الاحتفاظ بالبيانات في نطاق سلطة قضائية محددة بسبب المتطلبات التنظيمية أو يكون لديهم ثقة بنظام قانوني محدد. يقترح بروفيسور Don Jerker B. Svantesson [238] أنه إذا كانت الخدمة تتم عبر الانترنت، فإن مكان الأداء غير مناسب كضابط إسناد.[239] إذا لم يتم تحديد موقع النشاط حيث يتم تخزين البيانات ومعالجتها، فلا يجب أن يكون ضابط الإسناد محل تنفيذ الأداء بالمعنى التقليدي للقانون الدولي الخاص و Brussels I Regulation.

يوجد أسلوب آخر يستخدم على نطاق واسع في إيجاد صلة مناسبة للإختصاص القضائي وهو وضع حدود (ring–fencing). وضع الحدود يقوم على فكرة أن الأعمال يجب أن توضح وتحد من أنشطتها التجارية إلى المواقع المرغوبة. ومن طرق هذا الأسلوب إضافة عبارة مكتوبة بشكل واضح في الشّروط والأحكام. ومع ذلك، إن البيان لا يخفف من مسؤولية المزوِّد. ففي الواقع، بعض مقدمي الخدمات السّحابية يفيدون في شروط الخدمة الخاصة بهم خدمة لبعض البلدان والإختصاص القضائي، في حين، من ناحية أخرى، لا تزال الخدمة نفسها في متناول الجميع تحت نفس الظروف بالنسبة للمستهلكين. أمّا الطريقة الثانية فهي استخدام تقنيات تحديد الموقع الجغرافي التي تمنع الوصول من مواقع جغرافية معينة بناءً على IP Addresses وتسمح بمراقبة مقدمي الخدمة مما يحد من التعرض للإختصاصات القضائية غير المرغوب بها. الطريقة الثالثة هي مطالبة المستخدمين المحتملين بالإفصاح عن بياناتهم الشّخصية ثم، بناءً على هذه المعلومات، تقدم الخدمة أو تقيّد. لم تثبت أي وسيلة أنها فعالة في حد ذاتها من الناحية العملية، وينصح بحراسة الحواجز من خلال النظر في جوانب عديدة من الأعمال، والمؤشرات الخاصة بكل بلد، متى كان ذلك ممكناً.[240] وبالتالي للحوسبة السّحابية خصوصية عندما يتعلق الأمر بالاختصاص القضائي والقانون الواجب التطبيق، وتطرح إشكاليات أكثر تعقيداً من التجارة الإلكترونية، إذ

---

[238] البروفيسور Don Jerker B. Svantesson مدير مشارك لمركز القانون التجاري في كلية الحقوق (جتمعة بوند) وشريك في المعهد السّويدي للقانون والبحوث المعلوماتية، جامعة ستوكهولم. وهو متخصص في الجوانب الدولية لمجتمع تكنولوجيا المعلومات، المجال الذي نشر عنه مجموعة من الكتب والمقالات، وقدم محاضرات في أستراليا وآسيا وأمريكا الشّمالية وأوروبا. .(https://au.linkedin.com/in/dan-jerker-b-svantesson-a4852b87)

[239] Dan Jerke B. Svantesson, PRIVATE INTERNATIONAL LAW AND THE INTERNET, 2007, p. 268.

[240] Dusko Martic: "Dispute Resolution for Cloud Services: Access to Justice and Fairness in Cloud-Based Law-Value Online Services", Eramus Mundus Joint International Doctoral Degree in Law, Science and Technology, 2017, p. 125-126.

إن خدمة الحوسبة تقدم وتنفذ عبر الانترنت كما سبق وذكرنا. فهل تكون وسائل حل النزاعات بالطرق الالكترونية حل أفضل للنزاعات التي قد تنشأ عن عقد الحوسبة؟

النبذة الثانية: حل النزاعات إلكترونياً

المفاهيم التقليدية لحل النزاعات الناشئة عن العقود الإلكترونية لا تتبع وتيرة تطور التكنولوجيا الجديدة. تطوير خدمات الحوسبة السّحابية أثار قضايا جديدة تختلف ما بين القانون الواجب التطبيق، الاختصاص القضائي، الطابع القانوني للنزاعات، حماية المستهلك... كما سبق وأظهرنا الجدل والمشاكل الحاصلة في هذا الإطار خاصةً عند عدم تحديد القانون والمحاكم المختصة في العقد، ويمكن أن يكون محدداً في العقد وسيلة من وسائل حل النزاعات بالطرق البديلة التي يمكن أن تكون وسيلة إلكترونية كالتحكيم الإلكتروني. فقد شهدنا في الآونة الأخيرة محاولات من عدّة هيئات عامة ومنظمات دولية لتطبيق الإطار القانوني لحل النزاعات بالطريقة الإلكترونية على الصّعيد الوطني والعالمي. مثلاً يمكننا ذكر "Le Cyber Tribunal" المنشأة عام 1995 من قبل University of Montreal للوساطة المجانية لجميع مستخدمي الإنترنت، ومؤسسة "Online Ombuds Office" التي تأسست عام 1996 من قبل Center for Technology and Dispute Resolution التابع لجامعة Massachusetts الأميركية. كذلك مركز الوساطة والتحكيم التابع للمنظمة العالمية للملكية الفكرية (WIPO) الناظر بالقضايا المتعلقة بالحقوق الفكرية. فيمكن إعتبار الولايات

المتحدة سبّاقة في هذا المجال، ففي عام 1996 أسس Jim Melamed & John Helie مركز المعلومات والموارد للوساطة (The Mediation Information and Resource Center (MICR)) على موقع www.mediate.com الذي تعود ملكيّته لشركة Resourceful Internet Solutions (RIS) المتخصصة في تطوير الإنترنت لمنظمات حل النزاعات؛ ومن ثم إدراكاً للحاجة الهائلة لحل النزاعات عبر الإنترنت، أنشأت شركة RIS شركة جديدة Online Resolution Inc للتركيز حصرياً على هذا التطور، كان مركزها في بوسطن وكانت ترتكز على التشغيل الكامل على الموقع www.onlineresolution.com الذي يقدم المشورة، الوساطة، التقييم والتحكيم عبر الإنترنت[241]؛ إلّا أنه توقف عن العمل عام 2003.[242] أمّا بالنسبة للإتحاد الأوروبي، فقد أصدر البرلمان الأوروبي بتاريخ 21 أيار 2013 تنظيماً بشأن تسوية المنازعات على الإنترت من أجل المنازعات

[241] John Helie & James C. Melamed: Online Dispute Resolution in the U.S, October 1998, published on mediate.com. (https://mediate.com/articles/ecodir1.cfm).

[242] http://www.onlineresolution.com (accessed on January 24, 2019 at 9:46 AM).

المتعلقة بالمستهلكين إلّا أنها لم تكن التجربة الأولى لأوروبا في الـ ODR، فكانت هذه التجربة قد بدأت منذ عام 2003، ومنذئذٍ أصبحت أوروبا السّباقة في هذا الموضوع مع الدراسات التي تقوم بها.[243]

ويجب ذكر مركز التحكيم الدولي لدى نقابة المحامين في بيروت الذي أنشئ عام 2015 والذي تضمن إمكانية إتمام التبليغات عبر البريد الإلكتروني أو عقد جلسات التحكيم بواسطة وسائل الإتصال المرئي والمسموع.[244]

لحل النزاعات بالطريقة الإلكترونية فوائد عديدة تعود على طرفي النزاع وخاصةً في ما يتعلق بعقود الحوسبة السّحابية، إذ إن خصائص الـ ODR تتلاءم مع خصائص الحوسبة السّحابية، فيمكننا المقارنة كالآتي:

- الخدمتان متوفرتان عند الطلب
- الخدمتان مرنتان
- الخدمتان تلقائيتان

إن السّرعة في توفير الخدمات السّحابية بحاجة للحصول على حلول للنزاعات بسرعة، وليس ملائماً تبادل المطالبات المكتوبة على الورق وإرسالها فعلياً لحل النزاعات المتعلقة بالخدمات عبر الإنترنت والتي قد تكون سريعة وكبيرة الحجم وأحياناً يمكن أن تكون على درجة عالية من التقنية.[245]

كما إن هذه الوسيلة هي أوفر تكلفة على المستهلك من الطرق التقليدية لحل النزاعات خاصةً عندما يكون محدداً في العقد اختصاص محاكم خارج مكان تواجد المستهلك كما سبق وذكرنا؛ وعندما يكون النزاع تقنياً يكون المحكمون الإلكترونيون عادةً ضليعين بالشّق التقني وأكثر تخصصاً فيأتي الحكم دقيقاً وبوقت أسرع من صدور الحكم التقليدي الذي يتطلب في هذه الحالات تعيين خبير، ووقتاً أطول إذ إن الإجراءات تكون طويلة.

أولاً، يجب تعريف الـ Online Dispute Resolution (ODR): إنه حل الخلافات خارج المحكمة، فهو امتداد للـ Alternative Dispute Resolution (ADR) وإذا ركزنا على جزء online أي عبر الانترنت، فنحدد ODR من خلال استخدام التكنولوجيا عبر الانترنت. أصبح مصطلح ODR شائعاً

---

[243] Marta Poblet and Graham ROSS: ODR in Europe.

(Available at: https:www.mediate.com/pdf/poblet_ross.pdf)

[244] صادر بين التشريع والإجتهاد، التحكيم بالتعاون مع مركز التحكيم لدى نقابة المحامين في بيروت، المنشورات الحقوقية صادر ، لبنان، طبعة أولى 2015، ص. 7 و269 وما يليها.

[245] Dusko Martic: Online Dispute Resolution for Cloud Computing Services, Law Science and Technology, Joint Degree EM program, IDT- Universitat Autonoma Barcelona, Bellaterra, Barcelona, 2017.

(Available at: http://amsdottorato.unibo.it/8261/1/MARTIC_DUSKO_tesi.pdf).

يشمل أي استخدام لتكنولوجيا المعلومات والإتصالات لحل النزاعات. أمّا بالنسبة لتعريف محدد، فالملاحظات الفنية التي اعتمدتها الأونسيترال تقدم تعريفاً لـ ODR كالتالي:

"a mechanism for resolving disputes through the use of electronic communications and other information and communication technology"[246]

أي أنها آلية لحل النزاعات من خلال استخدام الاتصالات الإلكترونية وغيرها من تكنولوجيا المعلومات والإتصالات. ولكن لا تزال أشكال الـ ODR قابلة للمقارنة إلى حد كبير مع الـ ADR التقليدية غير المتصلة بالإنترنت (التفاوض– التقييم المحايد المبكر– المصالحة – الوساطة – التحكيم).

فتعتبر الـ ODR إمتداداً للوسائل الموجودة مع استخدام التكنولوجيا وبالأخص أدوات التواصل عبر الإنترنت الذي يسمى بالطرف الرابع.

أمّا إذا أردنا التكلم عن الإطار القانوني الدولي لوسائل حل النزاعات بالطرق الإلكترونية، يمكننا التكلم عن عمل الأونسترال وعن إطار تنظيمي جديد معروف بالـ Privacy Shield، وعن التنظيم الأوروبي لـ ODR (EU ODR Regulation).

1. عمل الأونسترال

في دورتها الثانية والأربعين في نيويورك عام 2010، وافقت لجنة الأمم المتحدة للقانون التجاري الدولي (UNCITRAL) على أنه يجب إنشاء فريق عمل للقيام بالعمل في مجال تسوية المنازعات عبر الإنترنت المتعلقة بمعاملات التجارة الإلكترونية عبر الحدود. وحددت الأونسترال ولاية الفريق العامل الذي أطلق عليه اسم الفريق العامل الثالث (Working Group III) وذلك للعمل على القيمة المخفضة، ارتفاع حجم المعاملات الإلكترونية عبر الحدود وبما في ذلك المعاملات B2B [247] وB2C [248] واضعة في اعتبارها تأثيره على حماية المستهلك.[249]

هدف الأونسترال تأمين إطار قانوني دولي لتسوية المنازعات الدولية عبر الانترنت من خلال تطوير قواعد إجرائية لـ ODR بالإضافة إلى وثائق مكملة إضافية: مبادئ توجيهية للمحايدين، معايير دنيا لمقدمي ODR، قواعد تكميلية لمقدمي الـ ODR، مبادئ قانونية موضوعية لتسوية النزاعات وآليات التنفيذ عبر الحدود.[250]

---

[246] UNCITRAL's Technical Notes on Online Dispute Resolution, New York, 2017.

[247] B2B: Business to business

[248] B2C: Business to consumer

[249] http://www.uncitral.org/uncitral/commission/working_groups/3Online_Dispute_Resolution.html

[250] A/CN.9/WG.III/WP.112- Online Dispute Resolution For Cross-Border Electronic Commerce Transactions: Drafts Procedural Rules Preamble 2, Par. 3. (Available at: http://www.uncitral.org/uncitral/en/commission/working-groups/3Online_Dispute_Resolution.html)

لا يمكن اعتبار الملاحظات الفنية المتعلقة بحل النزاعات عبر الإنترنت الصّادرة عن الأونسترال والتي اعتمدتها الجمعية العامة في 13 كانون الأول 2016 إطاراً لـ ODR. ولكنها تعكس عمل الأونسترال ومحاولة إيجاد توافق في الآراء لإطار تنظيمي دولي عن ODR في التجارة الإلكترونية ولكنها ذات صلة بالعديد من الجوانب: تحدد عدداً من المبادئ والمقترحات المشتركة للقواعد التي يمكن أن تكون أساساً للأدوات القانونية المستقبلية التي تنظم ODR على المستوى الإقليمي أو الدولي كما وتوضح الإختلافات والقضايا في مناهج ODR من خلفيات قانونية مختلفة، وتؤكد ثقة الجمهور في ODR وفائدته.[251]

2. Privacy Shield

في تشرين الأول 2015 كما سبق ورأينا، أعلنت محكمة العدل الأوروبية بطلان إتفاقية safe harbor التي سمحت بنقل البيانات الشّخصية إلى الولايات المتحدة تحت مستوى مناسب من حماية البيانات. إثر قرار الإلغاء، بدأت المفوضية الأوروبية والحكومة الأميركية مفاوضات حول إطار عمل جديد ووصلوا إلى إتفاقية في شباط 2016.[252]

يقدم Privacy Shield تحسينات كبيرة مقارنة بقرارات Safe Harbour ولكن يظل هناك ثلاث نقاط رئيسية مثيرة للقلق تتعلق بحذف البيانات، ومجموعة البيانات الضخمة وتوضيح آلية أمناء المظالم (Ombdus person) الجديدة.[253]

اعتمدت المفوضية الأوروبية القرار بشأن إطار عمل Privacy Shield في 12 تموز 2016 وبدأ سريانه في اليوم ذاته، في حين وقع رئيس الولايات المتحدة على الأمر التنفيذي المعنوي "تعزيز السّلامة العامة" (Enhancing Public Safety) والذي ينص على أنه لن يتم تمديد حماية الخصوصية الأمريكية إلى غير المواطنين الأمريكيين أو المقيمين.[254]

---

[251] A/CN.9/WG.III/WP.140- Online Dispute Resolution For Cross-Border Electronic Commerce Transactions: Draft Outcome Document Reflecting Elements And Principles Of An ODR Process. (Available at: http://www.uncitral.org/uncitral/en/commission/working-groups/3Online_Dispute_Resolution.html) (Accessed on October 2, 2018 at 9:11 AM)

[252] http://ec.europa.eu/justice/data-protection/international-transfers/en-us-privacy-shield/index_en.htm (Accessed on February 28, 2019 at 12:45 PM).

[253] Chapter 5 of Opinion 01/2016 on the EU-US. Privacy Shield draft adequacy decision, the Article 29 Data Protection Working Party. (Available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf)

[254]http://ec.europa.eu/justice/data-protection/internationa-transfers/eu-us-privacy-shield/index_en.htm. (Accessed on February 29, 2019 at 14:00 PM).

في إطار هذا التنظيم، بموجب مبدأ "الرجوع والإنفاذ والمسؤولية"، يجب على الشّركات المشاركة تأمين حق الرجوع للأفراد المتأثرين بعدم الإمتثال للمبادئ الأخرى للتنظيم، وإتاحة الفرصة لمواضيع بيانات الإتحاد الأوروبي لتقديم شكاوى بشأن عدم الإمتثال من قبل الشّركات المعتمدة من قبل الولايات المتحدة ولإيجاد حل لهذه الشّكاوى إذا لزم الأمر بموجب قرار قضائي.[255]

يمكن للشخص المعني بالبيانات أن يشكو بشكل مباشر أو من خلال وزارة التجارة ويجب على الشركة/ المؤسسة/ المنظمة الرد على هذه الشّكوى خلال 45 يوماً كيف ستتعامل الشّركة مع المشكلة، وإذا لم يأتِ الرد حسب رغبة الشّخص يمكنه المراجعة بطرق أخرى. وفي إطار دراستنا، نرى أن هذا التنظيم لم يذكر تحديداً الطرق الإلكترونية لحل النزاعات، ولكنه يستتبع منطقياً أن تسوية النزاعات للحالات المتعلقة بعدم الإمتثال للمبادئ ستكون فعالة فقط إذا تم إجراؤها بشكل جزئي أو كامل من خلال أدوات الإتصال عبر الإنترنت. إلّا أن هذا التنظيم هو بين الولايات المتحدة والإتحاد الأوروبي.

3. EU ODR Regulation

نُظمت هذه المنصة في النظام الأوروبي رقم 524/2013 الذي كان الغرض منه تحقيق مستوى عالٍ من حماية المستهلك، والمساهمة في الأداء السّليم للسوق الداخلية وعلى وجه الخصوص بُعدَه الرقمي من خلال توفير هذه المنصة لتسهيل حلول مستقلة، غير متحيزة، شفافة، فعالة، سريعة ومنصفة للنزاعات بين المستهلكين والتجار على الإنترنت.[256]

EU ODR Regulation تسمح للمستهلكين والتجار في الإتحاد الأوروبي أو النرويج وأيسلند و Liechtenstein بحل النزاعات المتعلقة بمشتريات السّلع والخدمات عبر الإنترنت دون اللّجوء إلى المحكمة.

يستعمل لإرسال الشّكوى إلى هيئة معتمدة لتسوية المنازعات التي تكون منظمة محايدة أو فرد يساعد المستهلكين والتجار في تسوية النزاعات، تستخدم هذه المنصة فقط هيئات حل النزاعات التي وافقت عليها حكوماتها الوطنية لمعايير الجودة المتعلقة بالعدالة والشّفافية والفعالية وسهولة الوصول.

كما أنها منصة سهلة الإستخدام تأخذ المستخدمين من خلال عملية حل النزاع بطريقة تدريجية، وتوفر ترجمات بجميع لغات الإتحاد الأوروبي ولها حدود زمنية معينة لحل النزاع/ الشّكوى.

---

[255] 2.1. Privacy Principles (26) in Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-US Privacy Shield.

[256] Art. 1 of Regulation on consumer ODR (Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32013R0524)

وعليه، لإنشاء شكوى يجب أن يكون كل من المستهلك والتاجر متمركزين في الإتحاد الأوروبي أو النرويج وأيسلندا و Liechtenstein، فيملأ الطرف نموذج شكوى على الإنترنت ويرسله أو يتركه كمسودة ولكن لديه 6 أشهر لتقديم الشّكوى إذا قام بحفظها كمسودة وإلّا حذفت تلقائياً لأسباب تتعلق بحماية البيانات.

ثم بمجرد موافقة التاجر على استخدام إجراء حل النزاع لمعالجة الشّكوى، يكون أمام المشتكي 30 يوماً للإتفاق على هيئة تسوية النزاعات التي ستتعامل مع النزاع. وإذا مرّت المدة المحددة فلن تتم معالجة الشّكوى من خلال النظام الأساسي.

وبعدها ستتم معالجة الشّكوى، وإذا تمكنت الهيئة أو حتى إذا لم تتمكن من الوصول إلى حل بالنسبة للنزاع، سيتم إشعار مقدم الشّكوى من قبل النظام الأساسي.[257]

إلّا أن هذه الأنظمة القانونية قد لا تتلاءم دائماً مع طبيعة الحوسبة السّحابية، إذ إن العقود هي عقود إذعان يكون المزوِّد محدداً الشّروط وطرق حل النزاعات التي لا تكون قابلة للتفاوض وبالتالي في الإطار التنظيمي الأوروبي ODR مثلاً حيث لا يمكن للمستهلك إلزام المزوِّد بقبول هذه الوسيلة في حل النزاعات خاصةً إذا لم يكن محدداً في العقد، خاصةً وأن المزوِّد يكون قد اختار قانوناً وقضاءً لصالحه، فلن يدخل في الـ ODR إذا ما كان هناك حافز قويّ.

كما وأن معظم التنظيمات المتعلقة بحل النزاعات بالطرق الإلكترونية تربط عقود الخدمات بعنصر الدفع/الثمن، وذلك لا يطبق دائماً على عقود الحوسبة السّحابية، فقد تكون في أغلب الأوقات مجانية؛ وبالتالي يجب إعادة تعريف عقود الخدمات وعدم ربطها بهذا العنصر، إذ إن هذه الوسائل الإلكترونية هي أسهل وأقل تكلفة بالنسبة للطرفين.

ولعدم الوقوع في مشكلة تنفيذ القرار التحكيمي الإلكتروني، يجب تأسيس منصة عالمية لحل النزاعات الإلكترونية تكون ملزمة التنفيذ في الدول المشتركة فيها.

الفقرة الثانية: مسؤولية مزوّد الخدمة

إن دراسة مسؤولية مزوِّد الخدمة أساسية إذ إنها تظهر للمستخدم المستفيد من الخدمة بعض الضمانات عند إنتقاله إلى السّحابة، وتختلف مسؤوليته باختلاف طبيعة صفته وباختلاف طبيعة الخدمة التي يقدمها. فيمكن ذكر بعض الأفعال التي ترتب مسؤوليته كانقطاع الوصول إلى المعلومات أو مشكلة نقل المعلومات، عدم الإلتزام بقواعد الخصوصية، التعرض لمحتوى المعلومات... تختلف مسؤوليته من

[257] https://ec.europa.eu/consumers/odr/main/?event=main.home.howitworks. (Accessed on February 28, 2019 at 16:20 PM).

مسؤولية مدنية إلى مسؤولية جزائية إلى إنعدام هذه المسؤولية. لذلك يجب التطرق إلى ثلاث صفات: صفته كمقدم خدمة، صفته كمراقب/ضابط/متحكم بالبيانات وصفته كمعالج لهذه البيانات.

النبذة الأولى: مسؤوليته كمقدم خدمة

مقدم الخدمة مرتبط بعقد بالطرف المستفيد منها، وبالتالي إن أي خرق من قبله لأي بند من بنود العقد يؤدي إلى ترتيب مسؤوليته وتعتبر مسؤولية تعاقدية؛ وعناصر هذه المسؤولية كما في العقود المبرمة بالطرق التقليدية: وجود عقد صحيح، حصول خطأ، وقوع ضرر ووجود صلة سببية بين الخطأ العقدي والضرر.

أمّا بالنسبة للخطأ ففي إطار الحوسبة السّحابية نتكلم عن الخطأ الذي يقع بعدم بذل العناية المتوجبة لتحقيق بنود مستوى الخدمة ونوعها ومدى استمراريتها؛ ولكن هل يسهل على المستخدم الذي غالباً يكون غير متخصص تقنياً بإثبات التقصير أو عدم بذل العناية اللّازمة من قبل مهني؟ كما ويمكن لمقدم الخدمة إثبات عدم التنفيذ أو سوء التنفيذ الناجم عن خطأ ارتكبه العميل أو الناجم عن قوة قاهرة أو عن فعل الغير، وبالتالي لا يعد مسؤولاً عن الضرر الذي حصل فتنتفي مسؤوليته.[258]

وكثيراً ما تدرج بنود تنفي المسؤولية وتقيد التعويضات في الإطار التعاقدي مثلاً:

- شروط استخدام منصة Google Cloud

Clause 12: disclaimer: except as expressly provided maximum extent permitted by applicable law, google and its suppliers do not make any other warranty of any kind, whether express, implied, statutory or otherwise, including warranties of merchantability, fitness for a particular use and noninfringement. Google and its suppliers are not responsible or liable for the deletion of or failure to store any customer data and other communications maintained or transmitted through use of the services. Customer is solely responsible for securing and backing up its application, project and customer data. Neither Google nor its suppliers, warrants that the operation of the software or the services will be error-free or

[258] المادة 73 من قانون المعاملات الإلكترونية والبيانات ذات الطابع الشّخصي (2018/81):

"يسأل مقدم الخدمات التقنية تجاه عملائة عن حسن تنفيذ موجباته التعاقدية.

يجب أن تتضمن العقود الموقعة مع العملاء وملحقاتها تحديداً لمستوى الخدمة ولنوعها ومدى استمراريتها.

يعفى مقدم الخدمات التقنية كلياً أو جزئياً من المسؤولية إذا أثبت أن عدم تنفيذ العقد أو سوء تنفيذه ناجم عن خطأ ارتكبه العميل أو ناجم عن القوة القاهرة أو عن فعل الغير."

uninterrupted. Neither the software nor the services are designed, manufactured, or intended for high-risk activities.

بما معناه أن Google لا تتحمل المسؤولية عن حذف أو فشل تخزين أي بيانات تم الحفاظ عليها أو نقلها من خلال استخدام الخدمات؛ فيكون العميل وحده مسؤولاً عن تأمين ودعم تطبيقه ومشروعه والبيانات الخاصة به. ولا تضمن أن تكون الخدمة خالية من الأخطاء أو غير منقطعة.

Clause 13: Limitation of Liability

13.1. limitation on indirect Liability to the maximum extent permitted by applicable law, neither party, nor google's suppliers, will be liable under this agreement for lost revenues or indirect, special, incidental, consequential, exemplary, or puritive damages, even if the party knew or should have known that such damages were possible and even if direct damages do not satisfy a remedy.

13.2. Limitation on amount of liability. To the maximum extent permitted by….., may be held liable under this agreement for more than the amount paid by customer to google under this agreement during the twelve months prior to the event giving rise to liability.

13.3. Exceptions to limitations. These limitations of liability do not apply to violations of a party's intellectual property rights by the other party, indemnification obligations, or customer's payment obligations.[259]

أي وضع حد للمسؤولية للحد الذي يسمح به القانون المطبق على الحدث، عن الأضرار غير المباشرة أو الخاصة أو العرضية... كما وضع حد للتعويض كحد أقصى ما دفعه العميل لشركة Google خلال فترة الإثني عشر شهراً السّابقة للحدث. وأخيراً نصت على أنّ هذه القيود لا تنطبق على الانتهاكات التي تطال حقوق الملكية الفكرية لأحد الطرفين من قبل الطرف الآخر.

- iCloud Legal Agreement

IX. Disclaimer of warranties, limitation of liability

"… Apple does not guarantee, represent, or warrant that your use of the service will be uninterrupted or error-free, and you agree that from time to time apple may remove the service for indefinite periods of time, or cancel the service in accordance with the terms of this agreement.

---

[259] https://cloud.google.com/terms/. (Accessed on March 1, 2019 at 8:30 AM)

… Apple does not represent or guarantee that the service will be free from loss, corruption, attack, viruses, interference, hacking, or other security intrusion, and apple disclaims any liability relating thereto…"

Limitation of liability

"… You expressly understand and agree that apple and its affiliates, subsidiaries, officers, directors, employees, agents, partners and licensors shall not be liable to you for any direct, indirect, incidental, special, consequential or exemplary damages, including, but not limited to; damaes for loss of profits, goodwill, use, data, cost of procurement of substitute goods or services, ot other intangible losses (even if apple has been advised of the possibility of such damages), resulting from: (1) the use or inability to use the service, (2) any changes made to the service or any temporary or permanent cessation of the service or any part thereof; (3) the unauthorized access to or alteration of your transmissions or data; (4) the deletion of, corruption of, or failure to store and/or send or receive your transmissions or data on or through the service; (5) statements or conduct of any third party on the services, and (6) any other matter relating to the service."[260]

فحدت Apple من مسؤولية العديد من الأشخاص المتعلقين بها كموظفيها والمدراء والوكلاء… عن أي أضرار مباشرة أو غير مباشرة أو عرضية وذكرت على سبيل المثال عدّة أضرار ممكن أن تنتج عن:

(1) استخدام أو عدم المقدرة على استخدام الخدمة
(2) أية تغييرات تمت على الخدمة أو أي إيقاف مؤقت أو دائم للخدمة أو أي جزء منها
(3) الوصول غير المصرح به أو تبديل الإرسال أو البيانات الخاصة بالمستخدم
(4) حذف أو تلف أو إخفاق تخزين و/أو إرسال أو إستقبال أو نقل البيانات الخاصة بالمستخدم على أو من خلال الخدمة
(5) سلوك أي طرف ثالث في الخدمة
(6) أي مسائل أخرى متعلقة بالخدمة.

[260] https://www.apple.com/au/legal/internet-services/cloud-en-terms.html (Accessed on March 1, 2019 at 9:12 AM).

النبذة الثانية: مسؤولية متحكم ومعالج البيانات

المتحكم هو "شخص طبيعي أو اعتباري أو سلطة عامة أو وكالة أو أي هيئة أخرى تحدد وحدها أو بالإشتراك مع الآخرين."[261] وبالتالي هذا التعريف يظهر أنه قد يكون هناك أكثر من جهاز تحكم واحد في ما يتعلق بنفس البيانات الشّخصية؛ على المتحكم التأكد من أن معالجته للبيانات الشّخصية تتوافق مع بعض المبادئ؛ يجب معالجة البيانات الشّخصية بطريقة عادلة وقانونية، لأغراض قانونية ولفترة محددة[262].

أمّا المعالج فهو "شخص طبيعي أو معنوي أو سلطة عامة أو وكالة أو أي هيئة أخرى تعالج البيانات الشّخصية نيابة عن وحدة التحكم".[263] ولكن القانون اللّبناني 2018/81 لم يأتِ على تعريف كل من المتحكم والمعالج ولكنه عرّف معالجة البيانات في مادته الأولى كما أتينا على الذكر سابقاً، كما عرّف المسؤول عن معالجة البيانات ذات الطابع الشّخصي بأنه الشّخص الطبيعي أو المعنوي الذي يحدد أهداف المعالجة وأساليبها.

يمكن لمزوِّد الخدمة أن يكون متحكماً فقط ويمكن أن يكون معالجاً للبيانات، ولكن يمكن أن يستخدم المتحكم كياناً آخر لمعالجة البيانات الشّخصية نيابةً عنه مثلاً من خلال الاستعانة بمصادر خارجية للمعالجة مع متعاقد من الباطن (sub-contractor)؛ القانون اللّبناني 2018/81 ذكر في المادة 96 التي عددت المعلومات الواجب إيرادها ضمن التصريح الذي يجب أن يقدم إلى وزارة الاقتصاد والتجارة وفق المادة 95، بأن يتم ذكر الملتزم من الباطن أو المقاول الثانوي في حال وجوده؛ أي أن القانون ذكر هذه العلاقة. ولكن الـ GDPR وقبله الـ DPD تكلما عنها؛ فالمادة 28 (2) و(4) من الـ GDPR تتعامل مباشرةً مع الحالة التي يقوم فيها المعالج باشراك "معالج آخر" يمكن تسميته "معالج ثانوي" أو "معالج من المستوى الثانوي". فيجب اختيار معالج يوفر "ضمانات كافية" في ما يتعلق بتدابير الأمن الفنية والتنظيمية التي تحكم المعالجة، واتخاذ خطوات جدّيّة لضمان الإمتثال لتلك التدابير. هذه العلاقة يجب أن تحكم بعقد بين الطرفين ويجب أن يعمل المعالج على تعليمات المتحكم ويجب أن تتوافق مع ما يعادل الإلتزامات المفروضة على المتحكم بموجب هذا القانون. قد يقيد عقد وحدة تحكم المعالج استخدام المعالجات الفرعية ولكن إذا تم استخدام معالجات متعددة ومعالجات فرعية، فيجب ان تعمل جميعها وفقاً لتعليمات وحدة التحكم.[264]

---

[261] Article 4.7 of GDPR (https://gdpr-info.eu/art-4-gdpr/)

[262] المادة 90 من قانون 2018/81

[263] Article 4.8 of GDPR (httpsL//gdpr-info.eu/art-4-gdpr/)

[264] Article 28, EU GDPR, "Processor" (Available on: www.privacy-regulation.eu/en/article-28-processor-GDPR.html) (Accessed on March 2, 2019 at 10:05 PM).

وبناءً على ما تقدم ذكره وتمييزه بين متحكم ومعالج، من المهم اعتبار أي من مقدمي خدمة الحوسبة السّحابية هي وحدات تحكم وأي منها هي وحدات معالجة وأي منها ليست لا متحكم ولا معالج. كذلك، يمكن أن تعمل كجهاز تحكم لبعض عمليات المعالجة ولكن كمعالج لأخرى، لذا يجب تقييم وضعها إذ يترتب على كل منها مسؤولية.

كما ويمكن للمزوّد الإستعانة بمزوّد ثانوي أكان في ما يتعلق بالتحكم أو بالمعالجة، ويكون المزوّد الرئيسي إمّا شفافاً لدرجة إعطاء تفاصيل حول جميع مزوّديه الفرعيين إلى المستخدمين أو لا يعطي أيّة معلومة عن وجود هؤلاء ربما لأسباب تتعلق بالسّرية التجارية. كما أنه من غير الواقعي أن يلزم مقدمي الخدمات بتغيير الترتيبات التجارية الموجودة مسبقاً وتعديل العقود مع المزودين من الباطن ليعكسوا إلتزامات المزود في عقودهم مع كل مستخدم. قد لا يكون مقدمو الخدمات الفرعية الحاليون مستعدين للموافقة على اتباع "تعليمات" المستخدم أو قبول إلتزامات الأمان المتزايدة مع تحمل مسؤولية إذا تم إنتهاك "إلتزامات حماية البيانات" لأن البنية التحتية للمزوّد الفرعي قد تخدم عدّة مزودي سحابات لكل واحدٍ منهم عدّة مستخدمين خاصين بهم. فمن يتحمل المسؤولية عند حصول أي إنتهاك؟

بالعودة أولاً لوضع مزوّد الخدمة، فعندما يكون للمزوّد مستخدم فردي طبيعي كعميل له، فمن المرجح أن يكون مزوِّد الخدمة "متحكم" في البيانات الشّخصية التي يتم جمعها والمتعلقة بذلك العميل.

إن بعض مزوّدي الخدمة السّحابية يعلنون عن صفتهم في ToS أي "متحكم" أو "معالج" في علاقتهم مع العميل. مثلاً "Apple" تنص في ToS لخدمة iCloud:

"You consent and agree to the: iCloud collection and use of certain information about you and your use of the service."[265]

أي "أنت توافق على جمع واستخدام معلومات معينة تتعلق بك وتتعلق باستخدامك للخدمة". وبالتالي يظهر جليًّا أنها وحدة تحكم لهذه البيانات.

بينما مزودون آخرون يتخذون موقفاً محايداً مما يجعله صريحاً في الحالات التي يكون فيها جهاز تحكم والحالات التي يكون فيها معالجاً؛ ففي ظروف مختلفة يمكن أن تختلف صفته.

يمكن بحسب تقسيم NIST لخدمات الحوسبة المذكور سابقاً تحديد صفة المزوّد:

- SaaS: فالمزوّد عادةً يقدم خدمات برمجية تهدف إلى معالجة البيانات ولديها القدرة على التحكم في البيانات المعالجة ومراقبتها، كما ويحدد كيفية معالجة هذه البيانات.

[265] https://www.apple.com/au/legal/internet-services/icloud/en/terms.html (Accessed on March 2, 2019 at 12:20 PM).

- IaaS: يقدم لعملائه فقط الأجهزة الإفتراضية أو البنية التحتية للحوسبة السّحابية، حيث يكون للعملاء حرية إتخاذ القرار كيف سيتم استخدام البنية التحتية المقدمة في حين أن المزوّد لا يعلم ما إذا كانت البنية التحتية تستخدم لمعالجة البيانات الشّخصية أم لا.
- PaaS: يمكن اعتبارها كخدمة مختلطة.

هذا التقسيم لا يؤثر على تقييم المزوّد كمعالج، إلّا أنه يؤثر بشكل كبير على مدى الترتيبات التعاقدية بين العميل والمزوّد خاصةً في ما يتعلق بإلتزامات ومسؤوليات الأطراف المتعاقدة.[266]

تختلف بالتالي مسؤولية المزوّد إذا كان متفقاً على أنه متحكم ولكنه قام بعمليات معالجة للبيانات الشّخصية أو سمح لطرف ثالث بالولوج إليها، ويمكن إعتبار هذا بحسب القانون اللّبناني 2018/81 في مادته 110 أنه ولوج غير مشروع إلى نظام معلوماتي خاصةً في العقوبة الثانية التي نصت عليها هذه المادة:

"الولوج غير المشروع الى نظام معلوماتي :

يعاقب بالحبس من ثلاثة اشهر الى سنتين وبالغرامة من مليون الى عشرين مليون ليرة لبنانية او بإحدى هاتين العقوبتين كل من اقدم، بنية الغش، على الوصول او الولوج الى نظام معلوماتي بكامله او في جزء منه او على المكوث فيه.

تشدد العقوبة الى الحبس من ستة اشهر الى ثلاث سنوات والغرامة من مليونين الى اربعين مليون ليرة، اذا نتج عن العمل الغاء البيانات الرقمية او البرامج المعلوماتية او نسخها او تعديلها او المساس بعمل النظام المعلوماتي."[267]

بالرغم من عدم استعمال المزوّد لطرق غير شرعية لوصوله إلى البيانات، فهو بسهولة تامة يمكنه الوصول إليها إلّا أنه يعتبر ولوجاً غير مشروع خاصةً أنه متفق مسبقاً في العقد بين الطرفين على صفة المزوّد أكان معالجاً أو متحكماً أو الاثنين معاً.

أمّا بالنسبة لمسؤولية المزوّد الثانوي، المعالج الثانوي أو من الباطن، فمسؤوليته يمكن أن تكون محددة بالعقد الذي يربطه بالمزوّد أو المعالج الرئيسي؛ فيمكن أن يعفيه من المسؤولية أم يحمله كامل المسؤولية أم تكون المسؤولية بحسب فعل كل طرف وتقصيره. إلّا أن صاحب البيانات يبقى المسؤول الرئيسي عن بياناته ولا يتوجب عليه التقصير بالحماية الذاتية بكل ما يتعلق به.

---

[266] Miroslav Chlopala & Stefan Pilar: Cloud Service Provider– Processor, Controller or both?, 31/08/2017 (Available on: https://cloudprivacycheck.eu/latest-news/article/cloud-service-provider-processor-controller-or-both/) (Accessed on February 26, 2019 at 15:23 PM).

[267] المادة 110 من قانون 2018/81.

خاتمة

مع ظهور الحوسبة السّحابية الحديثة، ظهر عدد لا يحصى من المصطلحات والمفاهيم والمناهج. على الرغم من أن الجميع تقريباً في قطاع تكنولوجيا المعلومات يتحدثون عن الحوسبة السّحابية، إلّا أن المفهوم لا يزال غير واضح بالنسبة للكثيرين. في هذه الرسالة قدّمنا مفهوماً للحوسبة السّحابية بالإستناد إلى تعاريف متعددة وصولاً إلى إستخراج تعريف تقني لهذه التكنولوجيا إذ إنها نموذج لنشر تكنولوجيا المعلومات يعتمد على المحاكاة الإفتراضية، حيث يتم نشر الموارد، من حيث البنية التحتية والتطبيقات والبيانات عبر الإنترنت كخدمة موزعة من قبل واحد أو أكثر من مقدمي الخدمات. بالإضافة إلى كونها عقداً غير مسمى يتم بين طرفين وغالباً ما يكون عقد إذعان ومقابل عوض.

الحوسبة السّحابية دخلت حياة الكثير من الأشخاص طبيعيين كانوا، معنويين أو حكوميين كما رأينا أعلاه ولعدّة أسباب تختلف من فئة إلى أخرى ومن شخص إلى آخر. فيمكنهم إختيار نوع السّحابة التي يريدونها وإبرام عقد مع الشّركة المزوّدة بالطرق الإلكترونية. هذه الشّركات المزوّدة كثيرة على الصّعيد العالمي إلّا إنه على الصّعيد الداخلي ليس هناك سوى شركة واحدة مزوّدة بالإضافة إلى بعض السّحابات التي تنشئها المصارف التي لا تزال غير معدّة لإستخدام العامة. هذا يظهر ضعف لبنان في إنشاء بنى تحتية سحابية وعدم إستفادة الدولة من هذا القطاع كغيره من القطاعات وقد أصبح بأهمية قطاع الكهرباء مثلاً. إن الأشخاص يعتمدون عليه خصيصاً عندما يريدون الإستعانة بمصادر خارجية لحفظ معلوماتهم؛ فلبنان يضيع فرصة قد تساعده على تحسين وضعه الإقتصادي، مثل اشتهاره بالسّريّة المصرفية يمكنه العمل على السّريّة السّحابية في لبنان وبين الدول العربية إلّا أنه متأخر جداً وعليه خوض مسيرة طويلة نسبياً بين بناء السّحابة والعمل على الأمان والسّريّة فيها، عندها يستطيع تطوير الحكومة بطريقة آمنة لتصبح حكومة إلكترونية أو حتى حكومة ذكية. هذا الموضوع يجب على الدولة أن تأخذه على محمل الجدّ خاصةً وأنه ليس بجديد فقد قدم إلى سيدر ولكن لم يكن دقيقاً وهو مشروع شراكة بين القطاعين العام والخاص.[268] ولكن هل سيرى هذا المشروع النور؟

المستخدمون يلجؤون للمزوّدين الأجانب لعدم توافر مزوّدين داخليين إمّا بطريقة مباشرة أو عبر سماسرة الذين يوجد العديد منهم في لبنان. تختلف الخدمات التي يقدمها السّمسار/الوكيل وبالتالي تارةً يكون وكيلاً وتارةً سمساراً.

على المستخدم عند إختياره مزوّد معيّن أن يتأكد من توافر شروط عديدة في الخدمة التي يقدمها وطريقة تقديمها. كما على المزوّد تطبيق معايير الحوكمة في تعاطيه مع الجمهور من شفافية ونزاهة، إذ عليه أن يكون شفافاً عند عرضه للخدمة فيمتنع عن الغش ويعمل بنزاهة أي يلتزم بالصّيانة والحفاظ على الخوادم

---

[268] إيلي الفرزلي: "الداتا سنتر: مشروع بلا جدوى إقتصادية؟"، الجمعة 8 شباط 2019، منشور على: www.al-akhbar.com.

والشّبكة. بموجب عنصر الصّيانة، يمكن مقاربة فكرة خدمة الحوسبة السّحابية بإيجار الصّناديق الحديدية المنصوص عنها في القانون والمنظم إيجارها كما يجب أن يكون الحال في خدمة السّحابة. وبالرغم من تملّصه من المسؤولية في أغلبية العقود التي يصوغها إلّا أنه يتوجب عليه تحمل المسؤولية أقلّه عندما يكون سبب الخلل أو الضرر واقعاً بفعل منه أو إهمالاً أو تقصيراً بموجباته. بالتالي عند بحث المستخدم عن المزوّد الذي يريد التعامل معه وتسليمه بيانات مهمّة ودقيقة وذات قيمة إقتصادية، عليه البحث عن الصّفات التي سبق ذكرها: الأمان، السّريّة والنزاهة.

يجب دراسة العقود المبرمة مع مقدم الخدمة كما والبنود المنصوص عنها والبحث عن تجارب الأشخاص التي تتعامل مع هذه الشّركة وعن مصداقيتها بتطبيق SLA وTOS التي تضعها. خاصةً أن التعاقد في هذه الخدمة يختلف عن التعاقد التقليدي، فهناك عقود نموذجية موضوعة مسبقاً لا يمكن للمتعاقد الضعيف التفاوض عليها؛ إلّا أن هذا الأخير يتمتع بحماية تختلف بحسب الدولة التي ينتمي إليها أو التي ترعى العملية التي قام بها، فالحماية في الإتحاد الأوروبي أهم من الحماية في القانون اللّبناني مثلاً.

قد يتعرض المستخدم للعديد من الهجمات أو الخروقات لخصوصيته وللبيانات التي كان يرغب أن تحفظ بأمان. يمكن أن تكون هجمات خارجية أي من قبل أطراف ثالثين من خلال الإختراق (hacking) أو من قبل دخول الطرف المقابل أي المزوِّد أو أحد التابعين له إلى حسابات المستخدم وبياناته. بالإضافة إلى ما هو أشد خطورة ممّا سبق ذكره وهو إمكانية الدول خاصةً الكبيرة منها الحصول على البيانات من خوادم تتواجد في دول أخرى كما الحال مع الولايات المتحدة التي تقوم بوضع تشريعات وإتفاقيات تخوّلها الحصول على البيانات التي تريدها. هذا يتطلب من المستخدم إختيار المزوّد بذكاء كما يتطلب توعية إلكترونية، توعية سحابية، توعية على المخاطر التي تواجه هذه التكنولوجيا، وحقوق وواجبات المستخدم التي يحميها قانون بلده.

الكثير من الناس قد تنعدم لديهم المعرفة التقنية سواء لعدم تعمقهم في هذا الموضوع والعوائق التي قد تنتج عن سوء الإختيار والإستعمال، بسبب إهمالهم أو مجرد استخدامهم للتقنيات والتطبيقات الجديدة دون معرفة الخطورة في مشاركة جميع بياناتهم الشّخصية، أو بسبب تعقيد الأمور التقنية وعدم إمكانية الجميع من استيعابها، وقد تجتمع في شخص واحد هذه الأسباب كلّها. يقع على الشّركات واجب تثقيف موظفيها والتابعين لها، وعلى الدولة تثقيف الموظفين التابعين لها في الدوائر. هذه التوعية يجب أن تكون بشكل دوري ومستمر وبطريقة مبسطة ليتمكن كل فرد من فهمها مهما كانت قدراته.

من جهة أخرى، لا تتوقف المسألة عند تأخر لبنان على الصّعيد التقني وإنما أيضاً على الصّعيد القانوني. فإذا تعرض المستخدم اللّبناني إلى أي إختراق أو أي نزاع بينه وبين المزوِّد لن يكون بإمكانه طلب الحماية من القانون اللّبناني. فالمشرع تأخر بإصدار قانون يتعلق بالمعاملات الإلكترونية وحماية البيانات حتى أواخر عام 2018، كانت خطوة مهمة ولكن متأخرة أظهرت أن التشريع اللّبناني لا يواكب التطورات والمستجدات. إلّا أنها خطوة خجولة إذ يشوب القانون بعض الثغرات تكلمنا عنها مسبقاً. لكن

توجّه لبنان من خلال خطوته الأولى نحو تنظيم هذا القطاع. يجب تعديل المواد التي تشوبها الثغرات أو سدّ هذه الأخيرة، كما يجب تفعيل هذا القانون بطريقة جديّة وإصدار مراسيم تطبيقية.

يمكن الإستعانة بالقوانين والأنظمة الأجنبية التي عمل عليها وعدلت عدّة مرّات لكي تتلاءم مع الواقع وتواكبه، خاصةً تنظيم الإتحاد الأوروبي المعروف GDPR والذي يعطي المواطن الأوروبي وكل شخص متواجد على الأراضي الأوروبية وبياناته الأولوية الحقّ في الحماية ويحمي النطاق الجغرافي الأوروبي من أيّة خروقات خارجية سواء من قبل الدول أو من قبل الشّركات. فمن حينها غيّرت بعض الشّركات سياساتها لكي تتطابق مع الشّروط التي يفرضها هذا النظام وإلّا يقطع الإتحاد علاقته معها. فقد رأينا أنّ عدداً كبيراً من المواقع تم حظرها لعدم إلتزام الشّركات بالشّروط المفروضة. الكثير من الشّركات اللّبنانية التي تتعامل مع الإتحاد الأوروبي تجري تعديلات لتتكيف مع الأنظمة السّارية، ومن هذه الشّركات مثلاً شرطة طيران الشّرق الأوسط التي تجري ندوات تدريبية لموظفيها، فقد نظمت فريقاً متخصصاً بالـ GDPR مؤلفاً من أشخاص ينتمون إلى جميع الفروع فيها. كما كرّس هذا النظام الحق في الخصوصية إلى أقصى درجاته وذلك بنصّه على إمكانية طلب النسيان عن المواقع الإلكترونية أو ما يعرف بالـ droit à l'oubli. لماذا لا تقوم جامعة الدول العربية بالأمر ذاته؟ أي تكرّس حقوق وخصوصية المواطن العربي أو من يسكن في النطاق الجغرافي العربي وتحمي المنطقة من أي خروقات خارجية في ما يتعلق بالبيانات؟

أمّا عند نشوء نزاع، يفرض على أطراف العلاقة تنفيذ بنود العقد الذي يربطها؛ وعند عدم نص العقد على طرق لحل النزاعات نلجأ إلى القانون الدولي الخاص والإتفاقيات التي تتعلق بموضوع النزاع مثلما رأينا سابقاً حيث يقع الخلاف بين محل إقامة المستخدم لتأمين الحماية الأضمن له إذ إنه الطرف الضعيف وبين محل تنفيذ موضوع العقد. إلّا أن الوسائل البديلة لحل النزاعات تبقى الأسرع والأحسن في حل مثل هذه النزاعات خاصة التحكيم وبطريقة أدق التحكيم الإلكتروني الذي يلائم الطبيعة الإلكترونية لهذه الخدمة، وهنا نقع في إشكالية القانون الذي يريد الفرقاء تطبيقه وقد يكون هؤلاء غير متفقين أو لا يتوصّلون لإتفاق. لذلك من الأفضل وضع إتفاقية موحدّة للعالم السّيبراني وكل ما يتم عبر الإنترنت يقع تحت أحكام هذه الإتفاقية فتنظم هذه الحياة الكثيرة التعقيد. يجب على الدول أن تتحد وتضع مثل هذه الإتفاقية وإنشاء منصّة لحل النزاعات بالطرق التي تلائم هذه العقود وهذه النزاعات ومن دون إدخال القوانين والإتفاقيات المتشعبة التي لا تزال في مكان ما لا تتطابق مع جميع النزاعات التي قد تنشأ.

هذا العالم كثير التشعبات والتعقيدات لا يقتصر فقط على التعدي على البيانات ذات الطابع الشّخصي إنما يشكل مكاناً لإرتكاب الجريمة مهما كان نوعها، فهذه البيانات الشّخصية قد تستخدم عند إختراقها لارتكاب جرائم أخرى كالتشهير والإبتزاز وغيرها، وهذا يشكّل موضوع دراسة آخر يحتمل التوسع والمقارنة خاصةً بعد التعديل الذي وقع على قانون العقوبات اللّبناني وغيره من النصوص التي يطالب البعض بتعديلها لكي تشمل الوسائل الإلكترونية.

من التوصيات التي يجب أخذها بعين الإعتبار:

1. على الصّعيد الداخلي

أ- على الصّعيد التقني

- تعزيز التوعية السّيبرانية والسّحابية من خلال الندوات والمؤتمرات المكثفة حسب الفئات ومعدل ثقافة الأفراد
- القيام بالدورات التدريبية لموظفي الشّركات والدوائر الحكومية لمعرفة أهمية الحماية والسّريّة وكيفية إستخدام التكنولوجيا الجديدة بطرق سليمة
- توظيف أشخاص متخصصين تقنياً في الدوائر الرسمية
- ضبط عملية حماية البيانات من داخل المؤسسات المعالجة بتفويض شخص بهذه الحماية، يكون على اتصال دائم مع الجهات المسؤولة
- العمل على بناء الحكومة سحابة خاصة بها
- التعاون بين القطاع العام والقطاع الخاص

ب- على الصّعيد القانوني

- العمل بالمبادئ واللّوائح الدولية
- تعديل القوانين لسدّ كل ثغرة فيها والعمل على تفعيل تطبيقها بطريقة جدّيّة وإصدار المراسيم التطبيقية
- تعديل القانون لكي يتطابق مع المواصفات الدولية المعمول بها خاصةً تلك المنصوص عنها في GDPR
- إنشاء سلطة مستقلة محدودة للإشراف على معالجة البيانات الشّخصية، وتنظيم هذه الهيئة في القانون المنشئ لها بحيث تتمتع باستقلالية تامة، مالية وإدارية وغير خاضعة لأية جهة حكومية خاصةً لوزارة الإتصالات. ووضع شروط لأعضاء الهيئة لكي يمارسوا وظيفتهم من دون تعارضها مع عملهم الآخر مثلاً عدم كون العضو صاحب مؤسسة عاملة في مجال معالجة البيانات. كذلك تنظيم عمل الهيئة وتحديد مهامها من إبرام إتفاقيات مع الجهات المعالجة الوطنية والخارجية؛ التأكد من مطابقة المعالجة مع القوانين؛ تلقي الشّكاوى؛ المحاسبة؛ تقديم المشورة والتوعية
- تفعيل التعاون بين الوزارات فلا جدوى لتعارضها

2. **على الصّعيد العربي**

- العمل في جامعة الدول العربية على نظام عربي يتعلق بحماية الحياة السّيبرانية وخاصة لتأمين الحماية للمواطنين الموجودين على أراضي هذه الدول وكل البيانات المحفوظة في هذه المنطقة على مثال النظام المعمول به في الإتحاد الأوروبي

3. **على الصّعيد العالمي**

- العمل على وضع إتفاقية تتعلق بالحياة السّيبرانية مثل مشروع إتفاقية جنيف الرقمية التي دعت إليها شركة ميكروسوفت وذلك لحماية الحياة الإلكترونية من القرصنة
- إبرام إتفاقية عالمية مرنة التطبيق في إطار الحياة السّيبرانية كتلك المتعلقة بالتحكيم لعام 1958 التي لا تزال تطبق حتى اليوم
- إبرام إتفاقيات ثنائية بين الدول الكبيرة التي توجد فيها الشّركات شبه المحتكرة لهذه الخدمة والدول الضعيفة في هذا المجال
- إنشاء platform عالمية لحل النزاعات إلكترونياً بعد توحيد قواعد العمل المطبقة في هذه النزاعات

عالجت هذه الرسالة حماية البيانات خاصةً الشّخصية منها على الصّعيد العالمي والدولي والمحلي؛ إلّا أن الحوسبة السّحابية والحماية لا تقتصر فقط على هذه البيانات لكنها تمتد إلى حماية حق المؤلف، حماية الملكية الفكرية... إذ إن الحياة الطبيعية أصبحت بكل ما بها حياة افتراضية تتطلب العناية والحماية القانونية أكثر فأكثر. ويطرح السّؤال إذا كانت هذه الحماية تختلف عن الحماية المعالجة في هذه الرسالة؟

مراجع

المراجع العربية

أ- المؤلفات

1. ابراهيم علي، العقود المسماة (البيع- الإيجار- الوكالة)، دار النشر مجهول، الطبعة الثالثة، 2012.
2. بدر أسامة، حماية المستهلك في التعاقد الإلكتروني، دراسة مقارنة، دار الجامعة الجديدة للنشر، الإسكندرية، 2005.
3. بدران عباس، عصر الفرص الجديدة: الحكومة الذكية، الدار العربية للعلوم الناشرون، 2014.
4. الجاف علاء، الآليات القانونية لحماية المستهلك في عقود التجارة الإلكترونية (دراسة مقارنة)، منشورات الحلبي الحقوقية، بيروت، الطبعة الأولى، 2017.
5. جبور فريد، حماية المستهلك عبر الانترنت ومكافحة الجرائم الإلكترونية (دراسة مقارنة) منشورات الحلبي الحقوقية، بيروت، الطبعة الثانية، 2012.
6. جميعي حسن، أثر عدم التكافؤ بين المتعاقدين على شروط العقد، دار النهضة العربية، القاهرة، 1991.
7. الحجازي رمزي بيدالله، الحماية المدنية للمستهلك بعد التعاقد الإلكتروني، منشورات الحلبي الحقوقية، بيروت، 2016.
8. صادر بين التشريع والإجتهاد، التحكيم بالتعاون مع مركز التحكيم لدى نقابة المحامين في بيروت، المنشورات الحقوقية صادر، لبنان، طبعة أولى، 2015.
9. صادق هشام، تنازع الإختصاص القضائي الدولي، دار المطبوعات الجامعية، الإسكندرية، 2002م.
10. عاليه سمير وعاليه هيثم، الوسيط في شرح قانون العقوبات "القسم العام"، المؤسسة الجامعية للدراسات والنشر والتوزيع، الطبعة الأولى، بيروت، 2010.
11. عيسى طوني، التنظيم القانوني لشبكة الإنترنت، صادر، بيروت، 2001.
12. محمد خليل خالد، حماية المستهلك في القانون الدولي الخاص، دار الجامعة الجديدة للنشر، الإسكندرية، عام 2009م.
13. ناصيف الياس، العقود المصرفية، منشورات الحلبي الحقوقية، الطبعة الثانية، بيروت، 2012.

ب- التقارير والتوصيات

1. الإتحاد الدولي للإتصالات: السّلسلة X: شبكات البيانات والإتصالات بين الأنظمة المفتوحة ومسائل الأمن، التوصية ITU-T X.1601، 2014.
2. الخوري جنان، الحوسبة السّحابية في الدول العربية، الجوانب القانونية والتشريعية واقع وآفاق، تقرير الاتحاد الدولي للإتصالات، بيروت، 2015.
3. مكتب وزير الدولة لشؤون التنمية الإدارية، سياسات وبرامج وإجراءات لخدمة عامة متميزة، التقرير السّنوي لعام 2014-2015.

ج- التشريعات والقوانين

1. إتفاقية بروكسل لعام 1968.
2. إتفاقية لوغانو لعام 1988.
3. الإعلان العالمي لحقوق الإنسان عام 1948.
4. التوجيه الأوروبي الصّادر في 20 أيار 1997 والمتعلق بحماية المستهلك في العقود المبرمة عن بعد.
5. تعميم مصرف لبنان رقم 2015/134.
6. الدستور اللّبناني الصّادر في 23 أيّار 1926.
7. قانون الأونسترال النموذجي بشأن التجارة الإلكترونية مع دليل التشريع 1996.
8. قانون اعتراض الإتصالات رقم 99/140.
9. قانون تنظيم قطاع الإتصالات رقم 2002/431.
10. قانون حماية المستهلك اللّبناني رقم 2005/659.
11. قانون الحق في الوصول إلى المعلومات رقم 2017/28.
12. قانون العقوبات اللّبناني رقم 43/340.
13. قانون المعاملات الإلكترونية والبيانات الشّخصية رقم 2018/81.
14. قانون الموجبات والعقود اللّبناني رقم 32/0.
15. قانون يرمي إلى صون الحق بسرية المخابرات التي تجري بواسطة أية وسيلة من وسائل الإتصال رقم 99/140.

د- **المحاضرات**

1. الأحمر جورج، العقود المدنية والتجارية، محاضرات في الجامعة اللّبنانية كليّة الحقوق والعلوم السّياسية والإدارية الفرع الثاني، خريف 2016-2017.
2. داغر إيلي، محاضرات في القانون المدني، الجامعة اللّبنانية كليّة الحقوق والعلوم السّياسية والإدارية، الفرع الثاني.

هـ- **الرسائل**

1. عبد العزيز الجمال سمير، التعاقد عبر تقنيات الإتصال الحديثة، (رسالة دكتورا) جامعة القاهرة، 2005.

و- **المقالات**

1. إيلي الفرزلي: "الداتا سنتر: مشروع بلا جدوى إقتصادية؟"، الجمعة 8 شباط 2019، منشور على al-akhbar.com.
2. علي أياد: الحوسبة السّحابية، البنك المركزي العراقي دائرة تقنية المعلومات والإتصالات، منشور على cbi-iq.
3. عمر محمد، ماهي تكنولوجيا الـ virtualization، 6 تشرين الثاني 2014، منشور على networks4ar.blogspot.com.
4. جريدة الأخبار: صحناوي تجسس على كل لبنان، 14 أيلول 2018، منشور على al-akhbar.com.

المراجع باللّغة الأجنبية

A. Books

1. Armbrust, Michael, Armando Fox, Rean Griffith, et al. 2009. Above the Cloud: A Berkeley View of Cloud Computing. Berkeley: EECS Department, University of California.
2. Bennett, K, P Layzell, D Budgen, et al. 2000, Service-based software: the future for flexible software. In Seventh Asia-Pacific Software Engineering Conference (APSEC). Singapore.

3. Boizard Maryline: "Le Droit à l'Oubli, Recherche réalisée avec le soutien de la Mission de recherché Droit et Justice", faculté de droit et de science politique Rennes 1, février 2015.
4. Christopher Millard: "Cloud Computing Law", Oxford University Press, The Several Contributors, 2013.
5. Dusko Martic: "Dispute Resolution for Cloud Services: Access to Justice and Fairness in Cloud-Based Law-Value Online Services", Eramus Mundus Joint International Doctoral Degree in Law, Science and Technology, 2017.
6. Dusko Martic: Online Dispute Resolution for Cloud Computing Services", Law Science and Technology, Joint Degree EM Program, IDT- Universitat Autonoma Barcelona, Bellaterra, Barcelona, 2017.
7. Elham Barjas & Hussein Mehdy: "Building Trust: Toward a Legal Framework that Protects Personal Data in Lebanon", SMEX, Beirut, 2017.
8. Freiberger, Paul, Michael Swaine. 2000. Fire in the valley: the making of the personal computer. 2. Ed. New York: McGraw-Hill.
9. Goldstine, H.H., A. Goldstine, 1946. The electronic numerical integrator and computer (ENIAC). Mathematical Tables and Other Aids to Computation.
10. Guide sur le Cloud Computing et les Data Centers, à l'attention de collectivités locales, sous la surveillance du ministère de l'industrie et du numérique francaise, juillet 2015.
11. K. CHANDRASEKARAN: "Essentials of Cloud Computing", CRC Press, US, 2015.
12. Maryke Silalah Nuth, "E-commerce Contracting: the effective formation of online contracts", University of Oslo, 2011.
13. Peter Mell, Timothy Grance: The NIST Definition of Cloud Computing, NIST special publication 800-145, September 2011.

14. Stiaram D & Manjuanth G: "Moving to the cloud: developing apps in the new world of cloud computing", 2012, Elsevier, USA.
15. Quemener (Myriam) & PINTE (Jean-Paul): "L'économie à l'ère numérique- in Cyber- Sécurité des acteurs économiques- risqué, réponses stratégiques et juridiques", 2013, Lavoisier, Paris.

B. Laws and guidelines:

1. A/CN.9/WG.III/WP.112- Online Dispute Resolution For Cross-Border Electronic Commerce Transactions: Drafts Procedural Rules.
2. A/CN.9/WG.III/WP.140- Online Dispute Resolution For Cross-Border Electronic Commerce Transactions: Draft Outcome Document Reflecting Elements And Principles Of An ODR Process.
3. Article 4 of the "Regulation (EU) 2016/679 of the European Parliament and of the council of 27 April 2016" on the protection of natural persons with regard to the processing of personal Data and on the free movement of such data, and repealing Directive 95/46/EC.
4. Article 29 Data Protection Working Party, Opinion 05/2012 on Cloud Computing, WP 196.
5. Clarifying Lawful Overseas Use of Data Act (CLOUD Act).
6. General Data Protection Directive (GDPR).
7. Guidelines governing the protection of privacy and transborder flows of personal data, published on oecd.org.
8. ISO/IEC DIS 17789:2014, Information Technology- Cloud Computing- Reference Architecture, 1st Edition, published on iso.org, 2014.
9. Office of the Minister of State for Administrative Reform: "Lebanese National Cyber Security Policy Guidelines", November 27, 2015.
10. Privacy Shield.
11. Regulation on consumer ODR.

12. UNCITRAL's Technical Notes on Dispute Resolution, New York, 2017.

C. Cases

1. Bertrand v. Ott [1978] ECR 1431, case number 150/77.
2. Google Spain and Inc. v. Agencia Espanola De Protection De Datos (AEPD) and Mario Costeja Gonzalez, C-131/12 (2014).
3. In re. DoubleClick Inc. Privacy Litigation, No. 1352, 2000 U.S. Dist. LEXIS 1148.
4. Maximillian Schrems v Data Protection Commissioner, Judgment in Case C-362/14.
5. 983 F. Supp. 215 (1998): Timothy R. McVEIGH, Plaintiff, v. William S. COHEN, et al., Defendants, No. CIV. A. 98-116. United States District Court, District Columbia, January 26, 1998.
6. Supreme Court of the U.S. No. 17-2: United States, Petitioner v. Microsoft Corporation, On Writ of Certiorari to the U.S. Court of Appeals for the Second Circuit, April 17, 2018.

D. Articles

1. APRIL GLASER: "Another 540 Million Facebook Users' Data Has Been Exposed", 03 April 2019, published on slate.com.
2. Adrian Chen & 'G Creep: "Google Engineer Stalked Teens, Spied Chats (updated)", Gawker, September 14, 2010.
3. Bart Van Den Brande: "Right to be forgotten" limited to the EU territory?, January 17, 2019, published on siriuslegaladvocaten.be.
4. Burners-Lee, lim. Information Management: A proposal. World Wide Web Consortium, 1998-1989, available on w3.org.
5. Butler B (2013): Amazon Web Services Worldwide Public Sector Summit, Washington DC, September, 2013, published on d36cz9buwru1tt.net.

6. Carol M, Hayes and Jay P. Kesa: "Privacy, Law, and Cloud Services", published in Encyclopedia of Cloud Computing, John Wiley & Sons Ltd., United Kingdom, 2016.
7. Cash Card: "Report: Bank Data for Sale on the Dark Web Rise By 135% Every Year", August 3, 2018, published on deeptoweb.com.
8. Christine Drake: "Cloud Data Destruction: Is Your Old Data Still Accessible?", August 15, 2012, posted on trend micro.
9. Cogeco Peer 1: "Le Big Data: un nouveau défi pour l'hébergement en cloud et la sauvegarde des données", 12 avril 2012, publié sur cogecopeer1.com.
10. David Drummond: "Greater Transparency Around Governement Requests", Google Public Policy Blog, April 20, 2010.
11. Debbie Garside: Moving the Middle East to the Cloud: Why it is time to seize the opportunity, 21 November 2017, published on: cloudcomputing-news.net.
12. Delvaux (P.H): "Les contrats d'adhésion et les clauses abusives en droit belge, en la protection de la partie faible dans les rapports contractuels (comparaisons franco-belges)", L.G.D.J., 1996.
13. Domingo R. Tan: "Comment, Personal Privacy in the information age: Comparison of Internet Data Protection Regulations in the United States and the European Union", 21 LOY.L.A.INT'L & COMP. L.J.661, 666 (1999).
14. Driss Kettani and Bernard Moulin: E-Government for Good Governance in Developing Countries, New York and UK, Anthem Press, 2014.
15. Florian Chague: "Controlez l'utilisation de vos données personelles", 7 Septembre 2017, publié sur openclassrooms.com.
16. Fontaine (M): "La protection de la partie faible dans les rapports contractuels", Rapport de synthèse, comparaisons Franco-Belges, L.G.D.J., 1996.

17. Georges Labaki: "Le gouvernement electronique: visions et strategies pour le cas libanais", 2011, publié sur lebarmy.gov.lb.
18. Gestin: "Traite' de droit civil, les obligations, les contrats, formation, Adition Pris L.G.D.G, 1988.
19. Greenberg A., Hamilto J., Maltz D. & Palel P.: "The cost of a cloud: Research problems in data center networks", 2009, ACM SIGCOMM Computer Communication Review 39(1).
20. Guy Rosen: "An update on the Security Issue", October 12, 2018, published on newsroom.fb.com.
21. Ian Khan: "What is Blockchain Technology? A Step-by-Step Guide For Beginners, March 1, 2019 published on: blockgeeks.com.
22. ITG: First Ever on a National Private Cloud! Our Affiliates Cirrus and IMS Provided Saradar Bank with a Cloud Managed Platform to Run the Bank's Core Services, Beirut, December 4, 2017, published on: itgholding.com.
23. Jim Sweeney, Virtualization: An Overview, published in Encylopedia of Cloud Computing, John Wiley & Sons Ltd., United Kingdom, 2016.
24. John Helie & James C. Melamed: Online Dispute Resolution in the U.S, October 1998, published on mediate.com.
25. Jules-Henri Gavetti: "le CLOUD Act, une nouvelle loi qui renforce l'ingérence des autorités américaines sur les opérateurs de CLOUD des US", publiés sur lesechos.fr.
26. Justice Opara-Martins, Reza Shandi and Feng Tian: "Critical analysis of vendorlock-in and its impact on cloud computing migration: a business perspective", Journal of Cloud Computing: Advances, systems and applications (2016)5:4, DOI 10.186/s 1377-016-0054-z.

27. Kapil and Craig Hill: Cloud Network and I/O Virtualization, published in Encylopedia of Cloud Computing, John Wiley & Sons Ltd., United Kingdom, 2016.
28. Kashif Bilal, Osman Khalid, Sif Ur Rehman Malik, Muhammad Usman Shahid Khan, Samee U. Khan and Albert Y. Zomaya: "Fault Tolerance in the Cloud", published in Encylopedia of Cloud Computing, John Wiley & Sons Ltd., United Kingdom, 2016.
29. Kristen Korosec: "This is the personal data that Facebook collects-and sometimes sells", March 21, 2018, published on fortune.com.
30. Lamia El Badawi, le droit à l'oubli à l'ère du numérique, LA REVUE,, "le droit à l'oubli", Numéro 8, Septembre 2016.
31. Lanois P.: "Caught in the clouds: the web 2.0, cloud computing, and privacy?", Northwestern Journal of Technology and Intellectual Property 9, 2010.
32. Lisa Sampson: A Cloud Broker Can Be A Cloud Provider's Best Friend, published on: searchitchannel.techtarget.com, January 2012.
33. Luciano Floridi: "We Dislike The Truth and Love to Be Fooled", CYCEON, November 21, 2016.
34. Maria LaMagna: "The Sad Truth about how much your facebook data is worth on the dark web", June 6, 2018, published on marketwatch.com.
35. Mark Smiley: "Big Data in a cloud", published in Encylopedia of Cloud Computing, John Wiley & Sons Ltd., United Kingdom, 2016.
36. Mathias (Cabinet d'avocats): "Patriot Act: Enjeux, Cloud Computing et Accés aux données", 2015, published on avocats-mathias.com.
37. Matt Blaze at al.: "Minimal Key Lengths For Symmetric Ciphers to Provide Adequate Commercial Security", US Defense Technical Information Center, 1996.

38. Michael A., Armando F., Anthony HK, Andrew K, Gunho L, David AP, Ariel R, Ion S & Matei Z: "A view of Cloud Computing", 2010, Commun ACM 53(4):5058.
39. Mike Gault: "BlockCloud: Re-inventing Cloud With Blockchains", May 13, 2018, published on: guardtime.com.
40. Miroslav Chlopala & Stefan Pilar: Cloud Service Provider-Processor, Controller or both?, August 31, 2017, published on cloudprivacycheck.eu.
41. Monica Brink: The Ruling On Cloud Computing: Analysing the Legal Perspective, 17 February 2017, published on cloudcomputing-news.net.
42. Murfett Legal: "Blockchains- "The Most Important Invention Since The Internet Itself", 2017, published on murfett.com.au.
43. Nick Ismail: Why do Banking institutions no longer fear the cloud?, 22 May 2018, published on: information-age.com.
44. Nile Latham: "Too Big for his Breaches: CIA Ex-Chief Free as Scientist is Jailed for Same Offense", N.Y. Post, March 8, 2000.
45. Olivier Cachard: "La Regulation Internationale Du Marché Electronique", lgdj, 2002.
46. Pradeep Kumar Tiwari & Dri Bharat Mishra: "Cloud Computing Security Issues, Challenges and Solutions", IJETAE, August, 2012, Vol. 2, Issue 8.
47. Rachel K. Zimmerman: "The way the "COOKIES" Crumble: Internet Privacy and Data Protection in the Twenty-First Century", Legislation and Public Policy, vol 4:439, unknown publisher and publishing year.
48. Raj Kumar Chalse, Ashwin Selokar & Arun Katara: "A New Technique of Data Integrity for Analysis of the Cloud Computing Security", CICN 2013.
49. Raymond E.: "What is a Hacker?", 2010, published on catb.org.

50. Richard Beaumont: "GDPR Compliance Means Cookie Notices Must Change", November 3, 2016, published on cookielaw.org.
51. Robert Hillman: "Standard-form contracting in the Electonic Age", N.Y.U.L. Rev.429.2002.
52. SalesForce: Why move to the cloud? 10 Benefits of cloud computing, published on salesforce.com, 2015.
53. Sam Murugesan and Irena Bojanova, "Cloud Computing: An Overview", published in Encyclopedia of Cloud Computing, John Wiley & Sons Ltd., United Kingdom, 2016.
54. Sean Rhody and Dan Dunn: "Government Cloud", published in Encylopedia of Cloud Computing, John Wiley & Sons Ltd., United Kingdom, 2016.
55. Siddharla Rao, Savan Gujrathi, Mithun Sanghui & Shubham Shah: "Analysis on Data Integrity in Cloud Environment", OSR Journal of Computer Engineering e-ISSN: 2278-0661, p-ISSN: 2278-8727, Volume 16, Issue 5, Ver. IX (Sept-Oct. 2014).
56. Simon Bradshaw, Christopher Millard and Ian Wladen: 'Contracts for clouds: comparison and analysis of the terms and conditions of cloud computing services", center for commercial law studies, London, 2010.
57. Simon Brashaw, Christopher Millard and Ian Walden: "The terms they are A-changin'... watching cloud contracts take shape, the center for technology innovation", issue in technology innovation, 2011.
58. Simon Dumontel: "Faut-il avoir peur du CLOUD Act?", 25 Juin 2018, publié sur august-debouzy.com.
59. Sophie Meunier: "Comment le RGDP affecte-t-il les politiques de cookies?, 10 octobre 2017, publié sur itgovernance.eu.
60. Stephan Watts: Cloud Service Brokerages: How CSB's Fit in a Multi-Cloud World, published on bmc.com, August 21, 2017.

61. Stylianou, K.K.: "An evolutionary study of cloud computing services privacy terms", John Marshal Journal of Computer and Information law 27.
62. Suttan Aldossary & William Allen: "Data Security, Privacy, Availability and Integrity in Cloud Computing: Issues and Current Solutions", article published in International Journal of Advanced Science and Applications, Vol. 7, No. 4, 2016.
63. Talkin' Cloud: Cloud Services Brokerage Company List and FAQ, published on: channelfutures.com, March 13, 2015.
64. Taylor Armerding: "The 18 biggest data breaches of the 21st centure", unknown date of publishing, published on csoonline.com.
65. TechSoup: cloud computing: benefits and barriers for non profits & libraries, published on techsoup.com, 2012
66. Tim Mather, Subra Kumaraswamy & Shaed Latif: "Cloud Security and Privacy: An Entreprise Perspective on Risks and Compliance", Sebastopol, CA: O'Reilly, 2009.
67. Tod Haselton: "How to find out what Google knows about you and limit the data it collects", December 6, 2017, published on cnbc.com.
68. Unknown (Candidate Number: 8024): Drafting a Cloud Computing Contract, University of Oslo Faculty of Law, 2011.
69. Vijay Kumar: "Powerful Uses of Cloud Computing", February 24, 2018, published on klientsolutech.com.
70. W. Kuan Hon, Christopher Millard & Ian Walden: "Negotiating Cloud Contracts: Looking At Clouds From Both Sides Now", Stanford Technology Law Review, Volume 16, Number 1, Fall 2012.
71. W. Kuan Hon, Christopher Millard & Ian Walden: "The Problem of "Personal Data" in Cloud Computing– What Information is Regulated? (The Cloud of Unknowing, Part 1)", Queen Mary University of London, School of Law, Legal Studies Research Paper No. 75/2011, 10 March 2011.

72. Yle: "Finnish court issues precedent "right to be forgotten" decision for Google to remove data", published on yle.fi, August 17, 2018.

المواقع الإلكترونية

1. alfa.com.lb
2. apple.com
3. ar.smex.org.
4. assets.documentcloud.org
5. citeseerx.ist.psu.edu
6. cloud.google.com
7. cnil.fr
8. coindesk.com
9. dawlati.gov.lb
10. dictionary.cambridge.org
11. download.microsoft.com
12. ec.europa.eu
13. facebook.com
14. google.com
15. itgholding.com
16. ivision.fr
17. law.ox.ac.uk
18. mediate.com
19. moph.gov.lb
20. navlink.com
21. oecd.org
22. onlineresolution.com
23. privacy-regulation.eu
24. publicationadministration.un.org
25. sas.com

26. statista.com
27. touch.com.lb
28. un.org
29. uncitral.org
30. zeroandone.me

فهرست

القسم الثاني

المخاطر والعوائق التي تواجه الحوسبة السّحابية